UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ELLIOTT BROIDY and BROIDY CAPITAL MANAGEMENT, LLC, Plaintiffs, —*v.*— GLOBAL RISK ADVISORS LLC, GRA MAVEN LLC, GRA QUANTUM LLC, GLOBAL RISK ADVISORS EMEA LIMITED, GRA RESEARCH LLC, QRYPT, INC., KEVIN CHALKER, DENIS MANDICH, ANTONIO GARCIA, and COURTNEY CHALKER, Defendants.	19 Civ. 11861 JURY TRIAL DEMANDED

FIRST AMENDED COMPLAINT

Plaintiffs Elliott Broidy and Broidy Capital Management ("BCM"), by and through their undersigned counsel, bring this action against Defendants Global Risk Advisors LLC ("GRA LLC"), GRA Maven LLC ("GRA Maven"), GRA Quantum LLC, Global Risk Advisors EMEA Limited, GRA Research LLC, Qrypt, Inc., Kevin Chalker, Denis Mandich and Antonio Garcia (collectively, "GRA" or the "GRA Defendants,"), and Courtney Chalker (with GRA, "Defendants"), and allege as follows.

INTRODUCTION

1. Plaintiff Elliott Broidy is a civic-minded businessman who has long been a vocal critic of countries, like Qatar, that fund and harbor terrorists. Over the past 20 years, Mr. Broidy has donated his time and resources to government and private organizations focused on the

international war on terrorism. In recent years, Qatar, a wealthy Persian Gulf state, has become increasingly prominent in the sponsorship of terrorism, openly hosting organizations such as Al Qaeda, the Muslim Brotherhood, and the Taliban. Surprisingly, despite these notorious and quite public connections with terrorism, Qatar has embarked upon a strategy of gaining influence in Western nations, including the United States, through a campaign of retaining Western political lobbyists and operatives. These efforts have often employed illegal means, most prominently in Qatar's procurement of the 2022 World Cup through widespread bribery. In response, Mr. Broidy's work had more recently turned to bringing significant public condemnation to Qatar, including from the President of the United States and several Congressional leaders. This case is brought against Americans who, for hire, assisted Qatar's "dirty tricks" campaign against Mr. Broidy, one calculated to silence him and to serve as a chilling example to others of what happens to those who oppose Qatar.

2. The GRA Defendants, acting as members of an international criminal enterprise (the "Qatari-Funded Criminal Enterprise" or the "Enterprise"), and funded by Qatar, retaliated against Mr. Broidy by unlawfully hacking his email servers and misusing his confidential data to harm him in different ways, including distributing curated and manipulated content to the media in a manner designed to inflict maximum damage. The GRA Defendants and the Qatari-Funded Criminal Enterprise targeted Mr. Broidy and his company, BCM, to silence his criticisms of Qatar and, by the spectacularly public nature of the attack, to send a message to others who would similarly exercise their First Amendment rights.

3. Defendants are the world-class hackers who, primarily from their U.S. locations and with U.S. citizen hackers, illegally broke into the email servers of Mr. Broidy, his wife, his executive assistant, and BCM. They then distributed the hacked materials in a secure manner to

various media outlets, as directed by other members of the conspiracy, to inflict maximum damage on Mr. Broidy.

4. The Broidy operation was a continuation of a long-standing and lucrative relationship between Qatar and GRA, whereby GRA utilizes "astroturfing" (using seemingly real—but actually hollow—"think tanks" or "studies" to generate ultimately false "news" stories in legitimate media outlets), as well as experienced hackers, many with U.S. military and intelligence agency experience, for the benefit of Qatar, a terrorist-harboring foreign regime.

5. GRA's work for Qatar has included extensive, covert operations to help Qatar maintain its blatantly corrupt bid for the 2022 World Cup. Qatar used astroturfing and paid extensive bribes to win the privilege of hosting the 2022 World Cup. Nonetheless, years later, the bid was on the verge of being revoked upon the publication of Qatar's bribes and other unsavory conduct (such as using slave labor to build the infrastructure). GRA's role in the corrupt scheme included addressing this crisis by hacking and covertly neutralizing key FIFA officials, such as one who had referred to Qatar as a "cancer" on soccer and had pushed for the World Cup to be relocated. This was a precursor to the hacking, surveillance and attempted neutralizing of Mr. Broidy. GRA pursued other, related projects by which it promised Qatar complete visibility into the private communications of those challenging its hosting privileges. GRA earned over $100 million for this work.

6. Qatar also paid GRA tens of millions of dollars to hack, surveil, and denigrate an ambassador to the United States from the United Arab Emirates ("UAE"). Because he is among the most the politically connected foreign diplomats based in the U.S., the hacking and surveillance of the Ambassador also intercepted sensitive and private information of U.S. citizens, including high-ranking U.S. government officials. The UAE Ambassador's emails were

hacked by GRA and distributed to the media in an operation with striking similarities to the tactics GRA later used against Mr. Broidy.

7. The hack of the UAE Ambassador and the targeting of FIFA officials, like the later hack of Mr. Broidy, were part of what GRA referred to internally as "special projects," a highly compartmentalized segment of GRA's work involving secretive, illegal conduct. GRA was perfectly suited for this work because it employs former National Security Agency, Central Intelligence Agency, and U.S. Armed Forces personnel with extensive offensive hacking expertise, and because, through its successful work on World Cup matters, GRA had earned the trust of Qatari officials at the highest levels of government.

8. GRA's special projects were compartmentalized and kept as a tight secret, even within GRA. The special projects team interacted covertly with high-ranking Qatari officials that were referred to only by codenames, such as Shep, Mightier and Botany.

9. The Qatari official known as Shep, Ali al-Thawadi, is the Chief of Staff to the Qatari Emir's brother, and has long been GRA's primary contact. Shep oversaw both GRA's World Cup work and the Broidy hack. GRA provided Shep periodic in-person and written briefings about its information-gathering projects, which included sensitive personal information about American citizens. Phone records show that, in the weeks leading up to the Broidy hacks, Shep had multiple phone calls with one of the public relations professionals who were caught red-handed in text messages discussing the media campaign against Mr. Broidy.

10. Another Qatari official with whom GRA worked closely, named Ahmad Nimeh and referred to within GRA by the code name "Botany," is the principal of a company that worked alongside GRA on the World Cup projects and who was publicly reported to be part of the Qatar "black ops" team hired to undermine rival bidders (including the eventual runner-up,

the United States). Just weeks before the Broidy hacks, Botany's company paid at least $3.9 million to the public relations professionals in charge of distributing the Broidy emails that GRA obtained for them through hacking. Those lobbying and media placement experts identified to date are being sued in a parallel action in the District of Columbia. A motion to dismiss that action was denied on March 31, 2020.

11. The overarching purpose of Qatar's scheme against Mr. Broidy was stated plainly in a WhatsApp exchange between two of the defendants in the DC case: to put Plaintiffs in "Mueller's crosshairs" and ultimately, "make Broidy go away." These are the same two defendants who received the $3.9 million. When a negative story was published in the *Wall Street Journal* based on material GRA had stolen, another WhatsApp message between the two celebrated with the simple statement, "He's finished."

12. Mr. Broidy and BCM are not finished. They have not gone away, nor will they. They now seek to hold the Defendants, including GRA's CEO and chief operative, Kevin Chalker, accountable for the harm they knowingly and intentionally caused.

13. Mr. Broidy and BCM hereby bring several federal and state causes of action to remedy and prevent serious business and property injury, including invasion of privacy and other harms, caused by GRA's participation in this egregious scheme. Mr. Broidy and BCM are entitled to relief from GRA's unlawful conduct, as described below.

PARTIES

14. Plaintiff Elliott Broidy is a citizen of the United States and the State of California who resides in Beverly Hills, CA. He is the Chief Executive Officer and Chairman of BCM. Mr. Broidy is a prominent business and civic leader and a philanthropist who has actively served in leadership roles in the Republican Party and Jewish organizations. His advocacy against

terrorism and extremism in protection of his country is well known, as is his criticism of Qatar for sponsoring terrorists.

15. Plaintiff BCM is a venture capital investment firm. It is a single-member, limited liability company organized under the laws of the State of California with its principal place of business in Los Angeles, CA. Mr. Broidy is the sole member of BCM and resides in California.

16. Defendant Kevin Chalker is the founder and, at all times relevant to this First Amended Complaint, the Chief Executive Officer of GRA LLC. He is a citizen of the United States and is domiciled in the state of New York. Mr. Chalker has never registered as an agent of the State of Qatar under the Foreign Agents Registration Act ("FARA"). He is a former CIA officer who advertises his former CIA experience to obtain clients. In addition to his position at GRA LLC, Mr. Chalker is the director of Bernoulli Limited and Toccum Limited, which are shell companies formed in Gibraltar whose own publicly available financial statements show that they received at least tens of millions of dollars in the months immediately leading up to the attacks against Mr. Broidy. Mr. Chalker also holds a position of authority and control over all subsidiaries and affiliates of GRA LLC and serves as a director to additional shell companies associated with 57/63 Line Wall Road, Gibraltar, including but not limited to Pygon Holdings Limited, Wrafton Limited, AtlasTel Limited, Doraville Limited, Tactical Data Analytics Limited, Champlain Maritime Limited, TDA Europe Limited, and Technical Group Holdings Limited.

17. Defendant GRA LLC is a limited liability company formed under the laws of Delaware, with its primary place of business in New York, NY. GRA LLC has a branch office located at 1140 Connecticut Ave. N.W. Suite 1120, Washington, D.C. 20036-4007. It has not registered as a FARA agent of the State of Qatar.

18. GRA LLC wholly owns (a) Defendant Global Risk Advisors EMEA Limited ("EMEA"), a Gibraltar corporation, which registered a branch in Doha, Qatar on October 26, 2017; (b) Defendant GRA Maven, a military consulting firm which was founded by Mr. Chalker in 2016 and which is headquartered in Southern Pines, NC; (c) Defendant GRA Quantum, a full-service cybersecurity company which was founded by Mr. Chalker in 2015, and which maintains an office in New York, NY; and (d) Defendant Qrypt Inc., a Delaware-incorporated and New York-based full-service cybersecurity company run by Defendants Kevin Chalker and Denis Mandich, which was founded days after EMEA entered into a broad cybersecurity and surveillance contract with Qatar during the planning stages of the attack on Plaintiffs.

19. Defendant GRA Research, LLC d/b/a Tactical Data Analytics is a limited liability company formed under the laws of Delaware with an office at the same Washington, DC address as Defendant GRA LLC. It has also had a branch registered in Virginia since 2014, as well as an office in or near Reston, VA. Upon information and belief, GRA Research LLC is under common ownership with the other the GRA entities, and ultimately controlled by Defendant Chalker. Defendant Antonio Garcia, who served as GRA's Chief Security Officer, was also affiliated with GRA Research LLC.

20. Upon information and belief, the foregoing GRA entities and Qrypt were all utilized in the cyberattacks on Plaintiffs.

JURISDICTION

21. This Court has federal question subject matter jurisdiction pursuant to 28 U.S.C. § 1331. A number of Plaintiffs' claims arise under federal law, including claims under the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*; the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2) and (a)(5); the Defend Trade Secrets Act, 18 U.S.C. § 1832(a)(1) and (a)(5);

the Economic Espionage Act, 18 U.S.C. § 1831; and the Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1962(c) and § 1964.

22. This Court has supplemental jurisdiction pursuant to 28 U.S.C. § 1367 over Plaintiffs' other claims as they relate to the federal statutory claims in this action and form part of the same case or controversy under Article III of the U.S. Constitution.

23. Additionally, this Court has diversity subject matter jurisdiction pursuant to 28 U.S.C. § 1332 because Plaintiffs and Defendants are from different states and the amount in controversy exceeds $75,000, exclusive of interest and costs.

24. In connection with the transactions, acts, practices, and course of business described in this First Amended Complaint, Defendants, directly and indirectly, have made use of the means or instrumentalities of interstate commerce, of the mails, or of the means and instruments of transportation or communication in interstate commerce.

25. Defendants Kevin Chalker, Courtney Chalker, Denis Mandich, and Antonio Garcia are citizens of the United States. Defendant GRA LLC is a company incorporated under the laws of Delaware, with its headquarters located in New York. Defendant GRA Maven is a company incorporated under the laws of Delaware, qualified to do business in New York and maintains an office in New York. Defendant GRA Quantum is a company incorporated under the laws of Delaware, qualified to do business in Utah, and regularly conducts business within the state of New York. Defendant Global Risk Advisors EMEA Limited is incorporated under the laws of Gibraltar, is qualified to do business in New York, and regularly conducts business within the state of New York. Defendant GRA Research LLC is a company incorporated under the laws of Delaware, and regularly conducts business in New York. Defendant Qrypt Inc. is a

company incorporated under the laws of Delaware, and regularly conducts business within the state of New York.

26. The GRA Defendants were at all relevant times acting in concert, as agents of one another and co-conspirators, and with the subsidiaries of GRA LLC serving as mere departments of the parent company, performing functions that GRA LLC would otherwise perform on its own. The GRA Defendants, either in person or through one another as agents, transacted business in New York. Under New York CPLR § 302(a)(1), "a court may exercise personal jurisdiction over any non-domiciliary who ... in person *or through an agent* ... transacts any business within the state or contracts anywhere to supply goods or services in the state." N.Y. C.P.L.R. § 302(a)(1) (emphasis added). In addition, each of the Defendants is a member of a conspiracy where one or more conspirators engaged in overt acts in furtherance of the conspiracy in this District that would be sufficient to subject those conspirators to the Court's jurisdiction. Therefore, each of the Defendants is subject to the personal jurisdiction of this Court.

VENUE

27. Venue is proper in this judicial district under 18 U.S.C. § 1965(a) because Defendants GRA LLC and Qrypt, Inc. have their headquarters in New York City, Defendant GRA Maven maintains an office in New York City, Defendant GRA Quantum maintains an office in New York City, Defendant Kevin Chalker transacts business here, and a substantial part of the events giving rise to the claims occurred in New York City.

28. Alternatively, venue is proper in this judicial district under 28 U.S.C. § 1391(b)(3), because there is no state in which all non-foreign defendants reside, and at least one defendant is subject to personal jurisdiction in New York.

FACTS

I. DEFENDANTS AND THE QATARI-FUNDED CRIMINAL ENTERPRISE TARGETED MR. BROIDY, STOLE HIS CONFIDENTIAL MATERIALS, AND DIRECTED A MASSIVE SMEAR CAMPAIGN AGAINST HIM

29. Because of Mr. Broidy's outspoken criticism of Qatar, the Qatari-Funded Criminal Enterprise identified him as a target and put into motion its sinister plan: to hack Mr. Broidy and BCM's confidential systems, steal his confidential materials, and then give those materials to public relations experts so they could inflict maximum damage.

A. Mr. Broidy Has Long Been an Opponent of Terrorist States and Became an Outspoken Critic of Qatar

30. Elliott Broidy is a staunch supporter of Israel and a recognized leader in conservative Jewish political circles. He has a long history of investing personal time and resources in anti-terrorist causes.

31. Mr. Broidy served on the Department of Homeland Security's Advisory Council between 2006 and 2009. There, he contributed to the report of the Council's Future of Terrorism Task Force, which called for the elimination of terrorist safe havens throughout the world. Mr. Broidy has long provided major funding for the Joint Regional Intelligence Center ("JRIC"), which is a cooperative effort between U.S. federal, state, and local law enforcement agencies to collect, analyze, and disseminate terrorism-related threat intelligence. The JRIC continues to serve as the Regional Threat Assessment Center for the Central District of California. Although Mr. Broidy is a committed Republican, his contributions in the area of anti-terrorism and America's national security have been widespread and bipartisan, including his efforts via the America Matters Foundation, American Freedom Alliance, the George Washington University Center for Homeland Security, the Hudson Institute, the Manhattan Institute of New York, the Pacific Council on International Policy, and the Panetta Institute for Public Policy.

32. In recent years, Qatar has risen to the forefront of terrorist sponsors, and Mr. Broidy has become its vocal critic.

33. Qatar is widely recognized as a sanctuary for terrorist leaders and organizations, including but not limited to Al Qaeda (including Al-Shabab and Al Qaeda in Syria, also known as Al-Nusra Front or Jabhat Al-Nusra), Hamas, the Taliban, and the Muslim Brotherhood. Indeed, the U.S. Department of Treasury has sanctioned numerous individuals residing in Qatar for raising funds for Al Qaeda. Qatar also has permitted Hamas leaders to operate freely within Qatar and has provided substantial funding to the group, despite the threat of international political and economic sanctions for such support. Similarly, Qatar has allowed the Taliban to operate and maintain an office in Doha since at least 2014. Qatar has given safe haven to many leaders of the Muslim Brotherhood after their expulsion from Egypt by the Egyptian government. And Qatar has allied itself in close strategic partnership with regimes governing Iran and Russia.

34. Mr. Broidy views Qatar as a major threat to U.S. security. He has funded public initiatives, such as conferences, to educate Americans about Qatar's support for terrorism.

35. Mr. Broidy also supported President Trump's 2016 political campaign, and once Mr. Trump took office in January 2017, Mr. Broidy continued voicing his strong concerns about Qatar at the highest levels of the U.S. government.

36. After taking office, President Trump criticized Qatar's role as "a funder of terrorism at a very high level" and made comments in support of an embargo against the state. In a June 2017 tweet, he criticized Qatar's "funding of Radical Ideology." And during a June 2017 Republican National Committee meeting, the President criticized Qatar for funding terrorism.

37. During that same month, Qatar's Middle Eastern neighbors were equally unnerved by Qatar's support for terrorist organizations. Saudi Arabia, the UAE, Egypt, Bahrain, and Yemen announced that they were cutting off diplomatic relations with Qatar, and blocking all land, air, and sea travel to and from Qatar.[1]

38. Qatar thus sought to influence U.S. policy in its favor through both legitimate and illegitimate means. Following the model for its success in procuring the 2022 World Cup, neutralizing critics was a key element of its U.S. effort. And, as in the World Cup, Qatar turned to GRA for support in hacking, surveillance, and using the resulting materials and astroturfing to denigrate and silence those whom the wealthy emirate viewed as potential threats.

39. Mr. Broidy's high-profile criticism of Qatar, and his apparent influence on the President, put him on a list of targets whom Qatar wanted neutralized.

B. The Qatari-Funded Criminal Enterprise Conspired to Target Mr. Broidy

40. As outlined below, the Qatari-Funded Criminal Enterprise perceived Mr. Broidy to be an enemy of Qatar and mobilized its members to neutralize him. Its objective was to reverse the Trump Administration's position on Qatar—which meant silencing Mr. Broidy and his associates.

41. GRA—as a member of the Enterprise with the unique and powerful skillset to conduct covert, offensive cyber and surveillance operations—conspired with public relations strategists to steal Mr. Broidy's confidential materials and plant carefully curated excerpts and manipulated materials with the press to cause Plaintiffs maximum damage.

[1] Anne Barnard & David D. Kirkpatrick, *5 Arab Nations Move to Isolate Qatar, Putting the U.S. in a Bind*, N.Y. Times (June 5, 2017), https://www.nytimes.com/2017/06/05/world/middleeast/qatar-saudi-arabia-egypt-bahrain-united-arab-emirates.html.

1. GRA Had the Unique and Specialized Skillset Necessary to Orchestrate and Execute Large-Scale Covert Cyber Operations

42. Since its founding, GRA's business model has been to sell decades' worth of U.S. covert operations training and surveillance skills for lucrative sums to foreign clients like Qatar (by far GRA's biggest client), regardless of the implications for Americans or American interests. As a member of the Qatari-Funded Criminal Enterprise, GRA contributed its unique, highly specialized skillset to manage and direct the covert cyberattacks on Mr. Broidy and BCM.

43. GRA is comprised of former intelligence, national security and military personnel trained in all levels of deception, disinformation, and cyber warfare. Founded and led by Kevin Chalker, a former CIA officer and cyberwarfare expert, GRA specifically employs experienced hackers from the intelligence and military communities. For example, former GRA employee John Sabin was identified by the *New York Times* two months before the start of the hack of Plaintiffs as "a former hacker for the National Security Agency,"[2] and was also described as "now a director of network security at GRA Quantum." That same October 2017 article ended with the implication that Mr. Sabin himself had actually already managed to circumvent some of the most advanced commercially available encryption technology, including for Gmail: "When asked if he had already circumvented physical multifactor authentication devices like Google's keys, Mr. Sabin would offer only: 'No comment.'" GRA's team members have designed classified government networks and led network security programs in the highest levels of the U.S. intelligence community. They have conducted operations to identify, track, monitor, and

[2] *See* Brian X. Chen & Nicole Perlroth, How Google's Physical Keys Will Protect Your Password, N.Y. Times (Oct. 25, 2018), https://www.nytimes.com/2017/10/25/technology/personaltech/ google-keys-advanced-protection-program.html. In addition, GRA's Managing Director of its London office, Roy Wilson, is a former covert officer in the CIA's clandestine service, and its former Managing Director of its Washington, DC office, Will Rankin, is a former top CIA expert on illicit finance.

seize illicit networks. Simply put, they are experts in the tactical collection of hard-to-access information.

44. Indeed, GRA holds two patents related to resonant cryptography—a system Mr. Chalker co-invented as a method for the secure transmission of data across any network. The patent applications are premised on Mr. Chalker's hacking expertise. Mr. Chalker's own filings showcase his deep understanding of system vulnerabilities to "brute force attack" (cracking a password or other security feature by automated, trial-and-error mechanisms) and argues in one application that it is a "profound understatement" to say that "the current security architecture is woefully inadequate."[3] That filing further explains that "[c]omplex systems break and are compromised in complex ways rarely understood or appreciated by their naïve makers. The essence of modern day hacking is based on this principle and only grows with technical complexity . . . ."[4]

45. Chalker's patent argues that no current system is safe from well-funded hackers:

> The battle to make devices/hardware/software perfectly secure has already been lost. The signature based tools of firewalls and antivirus software have failed because they cannot predict the future profile of infections. . . . **[I]f your company is a priority target entity at all costs, say by a determined and well-funded state actor, escalating resources will be deployed to break into the network normally reserved for the hardest targets**.[5]

46. And GRA makes no secret of its ability to use this expertise offensively to penetrate computer networks. GRA has advertised on its website its expertise with "penetration testing," which refers to hacking into a network to identify its security weaknesses. The

---

[3] US Patent No. 9,660,803, col. 2 ll. 63-67, col. 3 ll. 60-62. (issued May 23, 2017).

[4] *Id*. at col. 3 ll. 3-7.

[5] *Id*. at col. 4 ll. 6-22 (emphasis added).

underlying skills for penetration testing can be employed offensively or defensively. If an entity has hired an outside consultant to help identify its weaknesses, it is considered a "white hat" operation that is being used defensively to help that entity shore up its security system. But if the entity did not grant that consultant permission to conduct "penetration testing" on its network, and the consultant penetrates the network anyway, it is the same skillset being used in a wholly different, and illegal, type of operation, commonly referred to as a "grey hat" or "black hat" operation.

47. As explained by a professional IBM hacker in a *New York Times* editorial:

> Those who commit computer crimes fall into two categories: "black hat" and "gray hat." A black hat is someone who hacks with malicious intentions (espionage, data theft), seeking financial or personal gain by exploiting vulnerabilities. A gray hat is someone whose intentions may not be malicious but lacks the permission to hack into a system. Whether a particular criminal is a black hat or a gray hat is simply descriptive of the motivation behind what has already been established as illegal activity. [6]

48. GRA's current website highlights case studies involving "penetration testing" and "pioneering military training."

49. In October 2015, GRA's website more explicitly marketed "Grey Hat + Penetration Testing" that described GRA's expertise in the exact sort of hacking techniques employed against Mr. Broidy and BCM:

> GRA's Grey Hat + Pen Testing (GHPT) service is a comprehensive suite designed to evaluate an organization's perimeter, public, and private network security. We utilize advanced techniques developed from years of expertise within the US government and private sector. These experiences include

[6] Charles Henderson, *Most Hackers Aren't Criminals*, N.Y. Times (Nov. 7, 2019), https://www.nytimes.com/2019/11/07/opinion/hackers-hacking.html

> penetrating the networks of America's adversaries, such as, terrorists and narcotics organizations.[7]

50. And in a 2015 video promoting GRA's Grey Hat service, GRA admits to having "advanced techniques to penetrate target networks," including private sector, private networks.[8] The video states that GRA employs both common attack methods to intrude into servers and, also, "uncommon and customized attacks," including custom "spear phishing" campaigns.

51. GRA's successful sales pitch to Qatar was even more explicit, specifically referencing teams of "white hat" operatives for legitimate work, and a separate (and larger) team of "black hat" operatives for the covert work, such as hacking and real-time electronic surveillance. As discussed below, GRA used a black hat technique—spear phishing—against Mr. Broidy's wife and his executive assistant to obtain their confidential BCM log-in credentials to accomplish the unlawful hacking.

2. The Enterprise's PR Strategists Identified Mr. Broidy To Be Silenced

52. In addition to the Defendants, the Qatari-Funded Criminal Enterprise includes public relations professionals with strong connections to members of the national and international media who can exert a powerful political influence. They include American lobbyists who have registered with the U.S. federal government to work as agents of Qatar. Several of them are defendants in Mr. Broidy's parallel lawsuit in the District of Columbia.

53. These well-funded PR strategists identified Mr. Broidy as a target and conspired with GRA to obtain the fruits of the successful hack for dissemination to the media.

---

[7] http://web.archive.org/web/20151002155106/http:/globalriskadvisors.com/; http://web.archive.org/web/20150830070535/http://www.globalriskadvisors.com/wp-content/uploads/Global-Risk-Advisors-Grey-Hat-Penetration-Testing.pdf

[8] Global Risk Advisors, *GRA GreyHat Penetration Testing Service*, You Tube (Oct. 28, 2015), https://www.youtube.com/watch?v=BLAYD64JxXQ

(a) Background of the PR Strategists

54. The PR strategist members of the Qatari-Funded Criminal Enterprise include, among others, Nicholas Muzin, Joseph Allaham, Gregory Howard, BlueFort Public Relations LLC, Spark Digital, Stonington Strategies, and Lexington Strategies.

55. BlueFort Public Relations LLC ("BlueFort) has a one-page website showing office addresses in Doha, London, and Washington, DC, but it is believed to be a shell corporation funded by Qatar. BlueFort's website indicates that Spark Digital (which shares the same Doha address) is an affiliate, effectively its alter ego. Spark Digital advertises itself as "the team that brought you the Qatar 2022 World Cup bid website and social media campaign."[9] Spark Digital's website was registered in 2011 by Ahmad Nimeh,[10] who was heavily involved in Qatar's corrupt bid for the World Cup, including the "black ops" aimed at secretly sabotaging

[9] https://www.slideshare.net/SparkDigi/spark-overviewdemo

[10] Former U.S. Ambassador to Qatar, Patrick Theros, is Nimeh's father-in-law. Theros' eponymous firm, Theros & Theros, LLP, is based at the same address Nimeh listed as the address in the domain registration of sparkdigi.com. This is also the same address where Brown Lloyd James ("BLJ"), a PR firm that undertook "an extensive campaign to undermine the 2018/2022 [World Cup] candidacies of competitor countries," had an office. *See* Dan Friedman, *Qatari Lobbyists Received Millions Through Shadow Firm*, Mother Jones (Jan. 8, 2019), https://www.motherjones.com/politics/2019/01/qatari-lobbyists-received-millions-through-shadow-firm/. Media reports indicate that ex-CIA agents from BLJ also helped disseminate propaganda against Qatar's rivals, by recruiting media members to hype negative stories, spy on rivals, and produce intelligence reports on key people. *See Exclusive: Qatar sabotaged 2022 World Cup rivals with 'black ops'; Whistleblower reveals ex-CIA agents and PR firm were hired in dirty tricks campaign that broke Fifa rules*, The Times of London (July 29, 2018). BLJ President, Michael Holtzman, emailed Nimeh during their employ stating, "For the past 4 months we have undertaken an extensive campaign to undermine the 2018/2022 candidacies of competitor countries, particularly Australia and the US." *Id.* Holtzman went on to detail the various black operations BLJ pursued, including "deliver[ing] several deeply revealing intelligence reports on individual targets that have been used internally by the bid." *Id.*

Qatar's rivals.[11] Mr. Nimeh has a close working relationship with GRA, so much so that GRA has given him a code name for purposes of their covert operations—"Botany."

56. Through all times relevant to this First Amended Complaint, Nicolas D. Muzin was the Chief Executive Officer of Stonington Strategies LLC, a public relations and lobbying firm incorporated under the laws of Delaware, and a political lobbyist who signed FARA documents on behalf of Stonington as a registered foreign agent for the State of Qatar. On August 24, 2017, he was retained by the State of Qatar for "consulting services," and on September 3, 2017, Stonington registered under FARA as a foreign agent providing "strategic communications" for the State of Qatar. Stonington Strategies has been reorganized into Stonington Global LLC, whose website states that "[i]n launching the new firm, Nick Muzin & his team plan to build on their success representing the State of Qatar."

57. Joseph Allaham was the co-founder of Stonington Strategies, where he served as partner for all times relevant to this First Amended Complaint. He has worked for Qatar, originally as an unregistered foreign agent until he eventually filed a registration statement under FARA on June 15, 2018, in response to a subpoena from Plaintiffs in a related action. He is also the CEO of Lexington Strategies.

58. Gregory Howard is a media placement expert, an agent who, through his relationships with members of the media, provides information and materials to the media to generate stories desired by the agent's client. In 2017 and 2018, Mr. Howard worked as a Vice President and Senior Media Strategist at the firm of Conover & Gould ("Conover"), based in Washington, DC. From July 2017 until January 18, 2018, Mr. Howard was a registered foreign

[11] David Gilbert, *Qatar accused of running "black ops" against rival World Cup bids*, Vice News (July 30, 2018), https://www.vice.com/en_us/article/ev8b7j/qatar-world-cup-2022-black-ops-rivals.

agent of Qatar through Conover. Beginning no later than May 10, 2018, Mr. Howard worked in Washington, DC, as Vice President of Mercury Public Affairs, a public strategy firm, which he left in April 2019. In each of his positions at Mercury, despite FARA filings that did not mention Qatar, Mr. Howard worked as a media placement strategist for Qatar.

(b) The Well-Funded PR Experts Told the Enterprise to Target Mr. Broidy

59. Qatar specifically retained Messrs. Muzin, Allaham, and Howard in an attempt to influence the Republican, American-Jewish community and other conservative supporters of the President, with the end goal of influencing White House policy. Their work included identifying Mr. Broidy and other Americans as critics to be silenced.

60. Mr. Muzin began working for Qatar sometime in 2017, and in late August of that year, the Qatari Embassy in Washington, DC, officially retained Stonington and Mr. Muzin to influence public opinion regarding Qatar. Their agreement specified that Mr. Muzin and Stonington were to provide "consulting services" including the "development and implementation of a government relations strategy for Qatar, as requested and directed by the Embassy."[12] The initial agreement that Mr. Muzin submitted to the U.S. Department of Justice provided that Qatar would pay Mr. Muzin and Stonington Strategies $50,000 a month for these services.[13]

61. The initial agreement further limited Mr. Muzin and Stonington Strategies from acting as "a representative, spokesperson or agent on behalf of the Embassy or the State of Qatar in any meeting or communication with any person, or in any public or private statement, or in any communications with the media" "[e]xcept as directed by the Embassy."

[12] https://efile.fara.gov/docs/6458-Exhibit-AB-20170903-1.pdf,

[13] *Id.*

62. The initial agreement instructed that Mr. Muzin and Stonington Strategies were "solely responsible for compliance with any applicable laws or regulations that govern[ed] [their] performance of" the agreement "including, without limitation, any laws in respect of taxation, registration as a foreign agent or lobbyist, or reporting as may be required by law."

63. Mr. Allaham also began working for Qatar in 2017, according to his initial FARA disclosures in his capacity as the CEO of Lexington Strategies.[14] According to his (subsequently filed) FARA registration, he worked directly for the Emir of Qatar, Sheikh Tamim bin Hamad Al Thani, and his brother Sheikh Mohamad bin Hamad Al Thani. (The Emir's brother is commonly referred to as "MBH.") GRA worked with these same individuals and referred to them for purposes of their covert operations by code names. The Emir of Qatar had the code name, "Apex." The Emir's brother, MBH, had the code name, "Mightier."

64. In the fall of 2017, in the weeks leading up to the attack, Mr. Allaham had five separate phone calls with MBH's chief of staff, Ali al-Thawadi. GRA also worked very closely with Mr. Thawadi and gave him the code name, "Shepherd," or "Shep," for short.

65. Mr. Muzin has admitted that he identified and described Mr. Broidy to the Qatari government as impediments to Qatar's foreign policy interests in the United States. In connection with his work for Qatar, Mr. Muzin or his employees or agents participated in weekly meetings at the Qatari Embassy in Washington, DC, where they discussed the ongoing efforts against Mr. Broidy. Mr. Muzin specifically mentioned Mr. Broidy in these meetings as an obstacle that needed to be dealt with for his lobbying on behalf of Qatar to succeed.

66. As plans for the upcoming hack were underway, increased payments flowed to these key public relations strategists. On December 15, 2017, shortly before the hacks on

[14] https://efile.fara.gov/docs/6563-Registration-Statement-20180615-2.pdf

Plaintiffs' computers began, Qatar gave a $500,000 balloon payment to Messrs. Muzin and Allaham's firm, Stonington Strategies, and increased the monthly retainer from $50,000 to $300,000.[15]

67. Even more significantly, BlueFort (led by Mr. Nimeh, the individual with GRA code name "Botany") paid at least $3.9 million to Stonington Strategies within a three-week-period, from late September to mid-October 2017, just weeks before the attacks.[16]

C. GRA Managed and Executed an Unlawful Scheme to Hack Plaintiffs' Computer Systems and Email Servers

68. For the execution of the hack, Qatar had the perfect firm on hand—GRA. GRA had both the skillset for hacking and had earned Qatar's trust through years of performing other, underhanded projects for Qatar that involved generating false, negative stories through astroturfing and cyber-hacking, most notably GRA's efforts related to Qatar's hosting the 2022 World Cup.

69. The Broidy hack fit within a broader, compartmentalized area of work GRA performed for Qatar, referred to as "special projects" (discussed more fully below). GRA segregated its special projects work because it was illegal and thus needed to be concealed from others within the company not inclined to engage in illegal activity, who were outside special projects. The funds for special projects were invoiced separately by Bernoulli Limited and

[15] https://efile.fara.gov/docs/6458-Exhibit-AB-20171221-2.pdf

[16] Mr. Muzin claims to have provided Mr. Allaham with $2.3 million of the $3.9 million. (Stonington filing: https://efile.fara.gov/docs/6458-Exhibit-AB-20171221-2.pdf). Separately, Mr. Allaham reported that Qatar paid him an additional $1.45 million at an unspecified date in "October 2017" through his company, Lexington Strategies, as an initial grant for promoting World Cup 2022. (Lexington filing: https://efile.fara.gov/docs/6563-Registration-Statement-20180615-2.pdf).

Toccum Limited, so as to conceal the illegal work from financial records of the other GRA entities.

70. One of the special projects involved hacking into private servers to spy on politically active American citizens seen by Qatar as potential threats to its interests, like Mr. Broidy. For purposes of the special projects, GRA's U.S.-based teams would regularly compile and synthesize the results of their hacking and other covert intelligence gathering and produce a glossy dossier which was transmitted to GRA's office in Doha and hand delivered to Shep every two to three months. The information GRA brought to Shep included highly personal information on American citizens.

71. While GRA had hackers in a number of locations, many of the GRA hackers working on this campaign were located in GRA Research LLC's offices in Northern Virginia. GRA broadly employed many former intelligence and Special Forces personnel with offensive hacking skills developed while in government service, with a large team in Northern Virginia that was referred to as the "Reston Group" and affiliated with GRA Research LLC. The Reston Group was centrally involved in many "special projects" hacking operations, including the hack of Plaintiffs.

72. The head of the Reston Group was a former CIA official with information security expertise. Other members in the Reston Group included a software engineer formerly with the military, a former member of the Army's special operations forces, and others with prior work experience in cyberwarfare. The Reston Group included one particularly trusted operative, Defendant Anthony Garcia, who was GRA's Chief Security Officer. Shortly after Mr. Broidy filed his first lawsuit arising from the hacks, Mr. Garcia—with the assistance of Defendant

Courtney Chalker (Kevin Chalker's brother)—electronically "wiped" and then physically destroyed the electronic evidence in Northern Virginia and New York related to the hacking.

73. In furtherance of the conspiracy to neutralize Mr. Broidy, Defendants (including employees and contractors in the Reston Group) agreed to engage in, and did in fact manage and execute, a series of cyberattacks and other misappropriation of Mr. Broidy's private communications and documents. The purpose of the hacks was to obtain access to Mr. Broidy's confidential documents so that they could be manipulated and strategically disseminated to damage Mr. Broidy economically and as a spokesperson for opponents of Qatar's support of terrorism.

74. Upon information and belief, Mr. Chalker directed the activity of all the GRA Defendants, who acted in concert with one another, in furtherance of a common objective.

75. The GRA Defendants were able to hack into and steal Mr. Broidy's confidential communications by conducting successful, customized "spear phishing" campaigns, the first of which began on December 27, 2017. Spear phishing is the use of a fraudulent electronic communication targeted towards a specific individual, organization, or business in order to steal data or install malware on a targeted user's computer. On information and belief, Mr. Chalker celebrated the launch of the spear phishing campaign that very night, on Wednesday, December 27, 2017, by taking associates to the Sapphire Gentlemen's club in New York City.

76. In kicking off the effort against Plaintiffs, the GRA Defendants first targeted people who were close to Mr. Broidy—including his wife and his executive assistant—to obtain their respective log-in credentials to BCM's private server where the confidential documents were stored.

1. Defendants Targeted Mr. Broidy's Wife with Spear Phishing Emails

77. Robin Rosenzweig, a U.S. citizen, is Mr. Broidy's spouse and serves as legal counsel to Plaintiffs. Ms. Rosenzweig has an email account through Gmail, an email service provided by Google LLC ("Google"). Ms. Rosenzweig's Gmail account contains private communications and required at least a username and password for access.

78. On December 27, 2017, the GRA Defendants sent Ms. Rosenzweig an email to her Gmail account that appeared to be a security alert from Google. The email used Google trademarks without the permission of Google, including the Google logo and the Gmail logo. Defendants sent it from a Gmail address, disguised to look like an authentic security alert from Google. The email purported to alert Ms. Rosenzweig that the security on her account had been compromised and that she needed to verify or change her account credentials.

79. The link in the spear phishing email was designed to appear as if it would direct Ms. Rosenzweig to a legitimate URL on Google.com, but (not readily apparent without viewing the underlying source code) the link was in fact a TinyURL link that directed her to a professionally designed website that was intended to trick victims into believing it was actually an authentic Google account login page. TinyURL is a redirecting service that provides shortened URLs that redirect a website visitor to the website associated with the longer, masked URL. It is known to be used by hackers and scammers to avoid detection and circumvent spam and malware filters. When Ms. Rosenzweig clicked the TinyURL link, she was redirected to a website that contained Google's logo and appeared to be an authentic Google account update page—but it was in fact a fraudulent login page.

80. That email was one of dozens of "spear phishing" emails that Defendants sent in an effort to gain unauthorized access to Ms. Rosenzweig's Google accounts, which include the full suite of Google's online products, such as Gmail, Google Drive, Google Calendar, Google

Contacts, and YouTube. Eventually, Ms. Rosenzweig relied on these fraudulent misrepresentations and input her confidential login information, which GRA then captured. Her Google accounts contained, among other things, personal emails, business emails and documents, signed contracts, attorney-client privileged communications and documents, attorney work product, usernames and passwords to access other non-Google accounts, including an email account on the computer network of Plaintiff BCM. Without authorization, the GRA Defendants used Ms. Rosenzweig's stolen credentials unlawfully to access passwords stored by Ms. Rosenzweig on Google's servers, in clear violation of Gmail Program Policies and Google's Terms of Service.

81. On or about January 3, 2018, the GRA Defendants used the "Mail.ru" service to access and modify Ms. Rosenzweig's Gmail account without her consent. "Mail.ru" signifies a Russian email service that publishes an app that can be operated by users physically located around the world, including in the United States, to send and receive emails on Mail.ru or other email services like Gmail. Here, the GRA Defendants used the "Mail.ru" to read, send, delete, and manage emails and other documents in Ms. Rosenzweig's Gmail account, without her knowledge or consent, which in turn enabled them to obtain her log-in credentials for the BCM server.

82. Indeed, the GRA Defendants even modified Ms. Rosenzweig's account settings so as to keep her from discovering that her email had been hacked. They arranged for emails containing "Mail.ru," "viewed," or "alert" to be marked as read and moved immediately to her trash folder. The GRA Defendants did this to ensure that any legitimate security alerts would not be viewed by Ms. Rosenzweig. And unbeknownst to Ms. Rosenzweig, on January 4, 2018, she received a true security alert—that went directly to her trash folder—notifying her that a user or

users of the Mail.ru app had obtained access to read, send, delete, and manage her Gmail account, all without her awareness or consent.

2. The GRA Defendants Targeted Mr. Broidy's Executive Assistant with Spear Phishing Emails

83. The GRA Defendants also targeted Mr. Broidy's Executive Assistant. She has a private Gmail account, which she uses to send and receive personal emails, including private communications. It requires at least a username and password to be accessed.

84. On or around January 14, 2018, just as with Ms. Rosenzweig, the GRA Defendants began to send the Executive Assistant spear phishing emails disguised as Google security alerts. As before, the emails bore Google trademarks used without Google's permission and were sent through Google's Gmail service in violation of Google's Terms of Service and Gmail's Program Policies.

85. One of the fake spear phishing emails contained a fictitious security alert with a picture of the Executive Assistant's face and part of the Executive Assistant's phone number. Defendants sent the email from a misleading Gmail account with the name "Gmail Account" and the email address noreply.user.secure.services@gmail.com, which had been drafted to look like an authentic security alert from Google. The email purported to alert the Executive Assistant that the security on the account had been compromised and that the Executive Assistant needed to verify or change the Google credentials.

86. When the Executive Assistant clicked on the link the GRA Defendants placed in the email, it directed her to an Owly address. Like TinyURL and Bitly, Owly is a redirecting service that provides shortened URLs that redirect a website visitor to the website associated with the longer URL. It is known to be used by hackers and scammers to avoid detection and circumvent spam and malware filters. Here, it redirected the Executive Assistant to a website

that appeared as if it were an authentic Google account login page—but it was a fake log-in page, whose sole purpose was to deceptively and unlawfully obtain victims' user names and passwords. Eventually, the Executive Assistant relied on these fraudulent misrepresentations and input her confidential login information, which GRA then captured.

87. Through their spear phishing attack, the GRA Defendants were able to obtain the Executive Assistant's login credentials to BCM's computer systems.

3. Defendants Used Stolen Log-in Credentials to Infiltrate BCM's Servers

88. Plaintiff BCM has an exchange server physically located in Los Angeles, CA, which allows BCM employees to send and receive business and occasional personal emails. Mr. Broidy, his Executive Assistant, and several other employees all have secure email accounts on the BCM server containing private communications that require at least a username and password for access.

89. At least as early as January 7, 2018, the GRA Defendants finally achieved sustained access to Robin Rosenzweig's Gmail account, including thousands of confidential, proprietary BCM files. On January 16, 2018, they succeeded in breaching the BCM server—just two days after their successful spear phishing campaign on Mr. Broidy's Executive Assistant.

90. The GRA Defendants and fellow co-conspirators maintained unauthorized and unlawful access to the BCM email server from January 16, 2018, until at least February 25, 2018. During this period, there were thousands of instances of unlawful and unauthorized access to corporate email accounts at Plaintiff BCM, including but not limited to those of Mr. Broidy and his Executive Assistant. The GRA Defendants accessed BCM's mail server, which is known to contain emails, attorney-client privileged information, private communications, corporate and

personal documents, copyrighted material, contracts, business plans, confidential and sensitive proprietary information, and trade secrets and other intellectual property.

91. The GRA Defendants and their co-conspirators had full access to such confidential, sensitive proprietary information, and trade secrets and other intellectual property, and stole at least hundreds, and likely thousands, of the documents contained on the server. On information and belief, U.S. political operatives provided, either directly or through intermediaries, the Defendants with search terms and other search logic to identify emails and other content of interest. From those documents, Defendants and PR professionals created specific, highly damaging narratives about Mr. Broidy, with the ultimate goal of silencing him and other Americans.

92. The GRA Defendants accomplished each of these intrusions with the use of stolen or altered credentials.

4. The GRA Defendants' Imperfect Disguising of their Intrusions into the Broidy and BCM Servers

93. The GRA Defendants' exploitation of BCM's mail server was carried out via thousands of Virtual Private Network and Virtual Private Server (collectively, "VPN") connections that obfuscated the origin of the attacks.

94. VPNs route internet communication through additional networks to hide the original source of the connection. Some of these VPN connections occurred via IP addresses assigned to and operated by U.S. companies, who in turn allow third parties to engage in internet-based activity through those servers. This creates privacy for the end user of a VPN, as other servers (such as those hosting websites or mail services, such as Hotmail or Gmail) will only detect the VPN's IP address, but will not know the actual IP address of the person utilizing the VPN. For example, many of the suspicious IP addresses associated with the intrusions into

the BCM server were assigned to Micfo LLC, a company headquartered in Charleston, SC, which is affiliated with PureVPN and Secure Internet, LLC, thus concealing the identities of the ultimate end users.

95. The spear phishing emails and hacking intrusions used wires to transmit signals across state lines. Approximately 90% of the IP addresses of VPNs involved in the documented, unauthorized access of the BCM system came from VPNs operating from U.S.-based VPN servers, with most of the remainder coming from VPNs operating overseas that were previously reported to be favored by criminal actors.

96. While the artifacts discovered during Plaintiffs' forensic investigation indicated that the cyberattack mostly employed VPN technology, Plaintiffs also discovered non-VPN IP addresses from Vermont (12 separate hacker logins from two different IPs) and Qatar (two hacker logins from the same IP).

97. In each instance, the identifiable IP address connections lasted only a few seconds and were immediately succeeded by VPN connections. This suggests that there was either momentary human error or that the accessing computer automatically connected to Plaintiff BCM's network before the VPN mask could be activated.

98. When the mask dropped, the IP addresses revealed that the hacks were coming from a hotel near Killington, Vermont (on February 12, 14, 15, 17, 18, 19, 22 and 24, 2018), an acupuncture parlor in nearby Wallingford, Vermont (on February 19-21, and 25, 2018), and—in two instances—Doha, Qatar (on February 14 and 19, 2018). Additionally, hackers accessed the Gmail account of Mr. Broidy's Executive Assistant from an IP address located at a restaurant and event space in the Harlem area of New York City on January 14, 2018.

99. On information and belief, the GRA Defendants and accomplices obtained access to the Wifi systems of the U.S. locations by physically visiting them, then obtaining access to the Wifi systems so that they could use those Wifi systems in the attacks, either from nearby or remotely from other U.S. locations, including Northern Virginia.

5. The GRA Defendants Reviewed and Packaged the Stolen Emails for Dissemination and Placed Them in the Hands of Third Parties

100. After unlawfully obtaining Plaintiffs' private communications, emails, documents, and intellectual property, the GRA Defendants and co-conspirators within the United States converted the stolen materials to PDF files and physical printouts for dissemination to third parties, including journalists. Most of the PDFs disseminated to third parties bear time stamps different from the Pacific Time Zone associated with the original documents—and instead bear time stamps from the Central and Eastern Time Zones of the United States, where Defendants were located at the time that they converted the emails to PDF format.

101. On February 24, 2018, members of the Qatari-Funded Criminal Enterprise registered the email address "LA.Confidential@mail.com." Mail.com provides free email addresses akin to Google's Gmail service. The GRA Defendants used this email address to unlawfully deliver Plaintiffs' stolen emails to journalists employed by U.S. media organizations. Defendants and their co-conspirators directed selected third parties, including media members, to this site to get copies of curated sets of the stolen documents.

102. The GRA Defendants used another unmasked IP address traced to the North Carolina Research and Education Network ("NCREN") and a server in Chapel Hill, NC—close to GRA Maven's Southern Pines, North Carolina offices—to deposit the PDF formatted electronic documents into the "LA.Confidential@mail.com" account during this time. NCREN provides broadband infrastructure to various public institutions in North Carolina, and the

particular IP address at issue is associated with a "guest" WiFi network at the University of North Carolina. This point of access for the conspirators' email is roughly an hour's drive from both GRA Maven's location and from the towns where GRA employees lived at that time.

103. On information and belief, one of Defendant Kevin Chalker's close aides, who was one of the few people trusted to handle "off-books" finances for Defendants' illegal conduct, was taking graduate classes during the relevant time frame on the campus of UNC-Chapel Hill, the very campus from which someone accessed LA.Confidential@mail.com at the time when that account was being used to send hacked email PDFs to the media.

104. The GRA Defendants also placed Plaintiffs' stolen emails on a website whose ultimate owner was concealed using Domain by Proxy LLC, a company that allows users to register websites without disclosing their personal information.

105. In some cases, to avoid later detection, the GRA Defendants or their co-conspirators handed printed hard copies of the PDFs to third parties, including members of the media.

D. The Qatari-Funded Criminal Enterprise Coordinated a Smear Campaign Against Mr. Broidy Using Hacked Documents

106. As noted above, GRA launched its cyberattacks in a manner designed to inflict the most damage on Mr. Broidy and BCM—by synchronizing its efforts with public relations experts whose contacts with mainstream media could potentially bolster the credibility of the stolen and manipulated content, and distribute it far and wide.

107. Messrs. Howard, Muzin, and Allaham were among the knowing conduits. After GRA's successful, massive theft, these public relations strategists worked their extensive contacts with reporters to generate multiple stories about Mr. Broidy based on the stolen materials. The volume and timing of when they were paid (from at least fall 2017 through at

least early 2018), as well as their contacts with the media even before the fruits of the hack were generated, show that they were acting in concert with GRA and the other members of the Qatari-Funded Criminal Enterprise.

1. The Qatari-Funded Criminal Enterprise Combined an Excerpt of Hacked Material With Forgeries to Further Smear Mr. Broidy

108. GRA's first intrusion was into the files of Ms. Rosenzweig, which included various legal documents bearing Mr. Broidy's signature. Even before amassing all of the Broidy emails for the broader media attack, GRA and its accomplices used the products of the hack to create forgeries in order to discredit Mr. Broidy.

109. Specifically, they used stolen materials to lend the appearance of legitimacy to a phony news story based on fabricated contracts packaged together, intending to smear Mr. Broidy by "revealing" unsavory business deals he never actually made. The first of the fabricated contracts purported to call for Mr. Broidy to provide political consulting services to a sanctioned Russian bank, VTB bank, and the second forgery purported to call for Mr. Broidy to manage $40 million in invested funds from the United Arab Emirates and from a Ukrainian bank, ICU. These contracts were entirely falsified, but the GRA Defendants packaged them with a third document—a genuine "Beneficial Owner's Declaration" signed by Mr. Broidy that, upon information and belief, GRA stole in the hack. The "Beneficial Owner's Declaration" had nothing to do with the fabricated contracts, or the business dealings reflected in them, but was added to lend credibility to the phony documents.

110. The metadata from the documents revealed that the fake contracts were created just days after Ms. Rosenzweig's Gmail account was accessed by GRA hackers in January 2018. Mr. Broidy's signature on the forged VTB contract appears similar to his authentic signature, and, upon information and belief, was lifted from hacked documents.

111. The purpose of creating the fake VTB contract was to suggest that Mr. Broidy was secretly and unlawfully helping a Russian bank under U.S. sanctions. The fake UAE contract was intended to create the false impression that Mr. Broidy's anti-Qatar advocacy was motivated by a secret business relationship with the UAE, and not his true concern for Qatar's sponsorship of terrorism.

112. The Qatari-Funded Criminal Enterprise tried to shop these documents to multiple media outlets in the United States but Mr. Broidy's representatives were successful in convincing those outlets that the documents were forgeries.

113. Because the Qatari-Funded Criminal Enterprise could not find any legitimate news media to publish stories presenting the forged documents as authentic, it resorted to publishing the materials in Qatar's state-owned media outlet, *Al-Jazeera*.

114. On March 7, 2018, *Al-Jazeera* published an article stating that Mr. Broidy is "under scrutiny over alleged deal with sanctioned Russian bank VTB," and speculated that the VTB contract "raises serious questions about whether Broidy is in breach of the US Foreign Agents Registration Act (FARA)." As for the contract involving UAE and the Ukrainian bank (ICU), the article claims it "expose[s] [Broidy's] connections with the UAE," and, further, claimed that Ukraine had begun a criminal investigation into Mr. Broidy's dealings.

115. This was all a complete fabrication, but GRA's hack provided the Qatari-Funded Criminal Enterprise with the ability to incorporate an electronic copy of Mr. Broidy's signature and to intersperse a genuine document among the fake ones, giving the lie a veneer of legitimacy. On information and belief, Defendants used their decades of combined professional experience in trickery and disinformation to skillfully architect and operationalize the effort to tarnish Mr. Broidy with mainstream media stories falsely claiming business ties to a sanctioned

Russian bank, the plain goal of which would was to make him a target of the Mueller Investigation. The fake story remains on Al-Jazeera's website today, along with copies of the forged documents.

2. Mr. Howard's Phone Records Show Repeated Contact with Key Reporters Who Wrote Stories Based on the Hacked Emails

116. Mr. Howard's phone records show that he orchestrated a sophisticated media and distribution campaign to place information illegally obtained from the hacking in the hands of journalists, media organizations, and public relations professionals.

117. Mr. Howard's phone calls following the hacking show that he was in close and frequent communication with journalists in the early months of 2018 before they began publishing stories that relied on information stolen from Plaintiffs' computer systems and servers. In some instances, Mr. Howard communicated with journalists for weeks before they published these articles. The intensity of those contacts often increased in the days prior to publication. During this same period, Mr. Howard closely communicated with public relations experts, research groups, and registered agents of Qatar to coordinate the media disinformation campaign against Mr. Broidy.

118. Starting on January 7, 2018, just hours after the first sustained hacker access of Ms. Rosenzweig's Gmail account (and thus hundreds of Plaintiffs' confidential documents), Mr. Howard engaged in a flurry of calls with his then-colleagues at Conover & Gould and outside public relations professionals, including someone closely affiliated with BlueFort.

119. From January 18 through May 22 of 2018, Mr. Howard participated in more than two hundred phone calls with reporters who contributed to stories regarding Mr. Broidy and Qatar or regularly covered Qatari-related issues. These included extensive, and at times, almost daily calls with now-former Associated Press ("AP") reporter Tom LoBianco, all leading up to

the time he authored several stories regarding Mr. Broidy in March and May, 2018, based on the contents of Mr. Broidy's hacked emails. In addition, in the same time frame, Mr. Howard conducted more than a dozen calls with the *New York Times*, *McClatchy*, the *Wall Street Journal*, and the *Washington Post*, all of which were focusing on stories regarding Mr. Broidy's hacked emails.

3. Messrs. Muzin and Allaham's Text Messages Show Their Calculated Effort to Distribute the Material and their Celebration of Damaging Mr. Broidy

120. As noted above, Messrs. Muzin and Allaham were in close contact with high-ranking members of the Qatari government (including GRA contacts Apex (the Emir), Mightier (MBH, the Emir's brother), and Shep (al Thawadi)) in the weeks leading up to the attack. Mr. Muzin then flew to Qatar within a few days of GRA's first successful hack into Plaintiffs' systems. Messrs. Muzin and Allaham's text messages with each other demonstrate their direct and prior knowledge of the hacking and their knowing use of stolen documents.

121. On January 25, 2018, shortly after GRA's successful hacking of BCM began, Mr. Muzin sent Mr. Allaham a message on WhatsApp, stating, "It's very good. . . . We got the press going after Mr. Broidy. I emailed you."

122. That same day, prior to the first public reports in the United States of materials stolen from Plaintiffs, Ben Wieder, a reporter for *McClatchy*, a Washington, DC publication focused on politics, emailed Mr. Muzin to tell him, "I'm working on a story about Elliott Broidy and was hoping to talk." Mr. Muzin, who was still in Qatar, forwarded this message to Mr. Allaham and commented, "Time to rock." Less than an hour after sending the email to Mr. Muzin, Mr. Wieder called Mr. Howard, and they spoke for more than 10 minutes. Mr. Wieder would go on to write extensively about Mr. Broidy on the basis of carefully curated emails and other documents stolen from Mr. Broidy's servers.

123. On March 1, 2018, the contents of emails stolen from Plaintiffs' computer accounts and servers appeared for the first time in media accounts. The *Wall Street Journal* credited its source as "a cache of emails from Mr. Broidy's and his wife's email accounts that were provided to the Journal."

124. Mr. Muzin shared the *Wall Street Journal* article with Mr. Allaham over WhatsApp that same day. Mr. Muzin then commented, "He's finished."

125. Other media outlets continued to publish more of the stolen emails, including the *Huffington Post* on March 2, 2018, and the BBC on March 5, 2018. The *Huffington Post* cited "[e]mails and documents an anonymous group leaked to HuffPost."

126. On March 13, 2018, Mr. Muzin remarked to Mr. Allaham via WhatsApp that recent news stories about Mr. Broidy have "[p]ut[] him in [M]ueller['s] crosshairs." This communication demonstrates one of the central goals of the Qatari-Funded Criminal Enterprise—to portray Mr. Broidy as a target of special counsel Robert Mueller's investigation.

127. That same day, Mr. Allaham wrote to Mr. Muzin on WhatsApp that a former U.N. official working under contract with the Qatari government, Jamal Benomar, had gone to Qatar prior to the date of the message "to get the emails. That what [*sic*] I think he was doing there [in Qatar]." Mr. Muzin responded by referencing Mr. Broidy by name.

128. On March 14, 2018, Mr. Muzin told Mr. Allaham on WhatsApp that he'd "get some intel about the Broidy event soon." This comment likely refers to a March 13, 2018, Republican fundraiser headlined by the President of the United States, for which Mr. Broidy had been listed as an event host.

129. The next day, on March 15, 2018, Mr. Muzin exclaimed to Mr. Allaham, via WhatsApp, "Elliott Broidy was not at the fundraiser!" The two were clearly excited at the prospect of having damaged Mr. Broidy's political standing.

130. Multiple additional news stories followed that expressly relied on the stolen documents. On March 21, 2018, the *New York Times* published a front-page article noting that an "anonymous group critical of Mr. Broidy's advocacy of American foreign policies in the Middle East" has been distributing "documents, which included emails, business proposals and contracts," belonging to Plaintiffs. On March 23, 2018, *Bloomberg* published an article about Mr. Broidy, which noted that it had "received two separate documents this week purporting to be versions" of materials belonging to Mr. Broidy.

131. On March 25, 2018, a front-page story in the *New York Times* reported extensively on Mr. Broidy's fundraising and business activities. The story reported that Mr. Broidy had agreed not to attend the March 13 fundraiser. The story was based, in part, on "[h]undreds of pages of Mr. Broidy's emails, proposals and contracts" received from what the *Times* euphemistically termed "an anonymous group critical of Mr. Broidy's advocacy of American foreign policies in the Middle East." This "anonymous group" is the Qatari-Funded Criminal Enterprise.

132. On March 26, 2018, *McClatchy* published a story authored by Ben Wieder that used hacked materials to denigrate Mr. Broidy, House Foreign Affairs Chairman Ed Royce, and the Congressman's wife, Marie Royce—just four days before the Senate was scheduled to vote on her appointment to be Assistant Secretary of State for Educational and Cultural Affairs. Also at that time, Chairman Royce's House Foreign Affairs Committee was attempting to advance H.R. 2712, known as the "Hamas Sanctions Bill," which specifically named Qatar as a sponsor

of Hamas subject to sanctions. It was only one of a series of articles hostile to Mr. Broidy authored by Mr. Wieder following contact with Mr. Muzin and Mr. Howard, who also had extensive communications with Mr. Wieder's editor, Viveca Novak.

133. And on May 4, 2018, in a WhatsApp message to Mr. Allaham, Mr. Muzin summed up the very obvious objective the Enterprise had pursued for months, stating: "our new friends can make Broidy go away altogether."

134. Media outlets in the United States and abroad threatened to publish—and continued to publish—materials stolen from Plaintiffs well into 2019.

135. GRA's extensive hacking and its intentional coordination with public relations professionals ensured that the Enterprise inflicted maximum damage on Mr. Broidy and BCM.

4. The Scheme Has Had Its Intended Effect of Damaging Plaintiffs

136. The overarching purpose of the scheme was to retaliate against Plaintiffs for Mr. Broidy's criticisms of Qatar. While the scheme has not succeeded in silencing Mr. Broidy, it has succeeded in causing great harm that, through this suit, Mr. Broidy seeks to remedy.

137. One element of this harm is that BCM has lost significant revenue and goodwill. BCM makes investments in, among other things, privately held defense contracting companies. In the defense contracting space, discretion is very important and highly valued. The projects of BCM portfolio companies involve sensitive counterterrorism and intelligence initiatives. The work is both highly confidential and proprietary. BCM clients rely on the company to protect information that is highly sensitive, and the fact that BCM was hacked—and that the fruits of the hack were spread through the media—has, quite predictably, caused counterparties and others to flee, and resulted in a substantial loss in business.

138. Mr. Broidy personally has been damaged in his broader business affairs, as business partners and others have not wanted to associate themselves with someone who,

following the press onslaught, had such high visibility. For example, investment and commercial banks with whom Mr. Broidy had long-term relationships suddenly ceased doing business with him, following the hacks and associated media campaign.

II. THE GRA DEFENDANTS' ATTACKS ON PLAINTIFFS ARE PART OF A PATTERN OF CYBERATTACKS ORCHESTRATED BY THE QATARI-FUNDED CRIMINAL ENTERPRISE

139. Defendants' attacks against Mr. Broidy and BCM were part of GRA's ongoing work for the Qatari-Funded Criminal Enterprise—work designed to neutralize the people and entities that Qatar perceives as threats to its geopolitical interests and overall standing in the international community.

A. The History of GRA's Covert Operations for the Qatari-Funded Criminal Enterprise

140. Over the course of its multi-year relationship with Qatar and the Qatari-Funded Criminal Enterprise, GRA has earned hundreds of millions of dollars by marketing and selling its hacking expertise in support of Qatar's corrupt regime. What began as corrupt efforts related to Qatar's tainted hosting of World Cup 2022 grew into a lucrative role in this criminal enterprise.

1. Mr. Chalker and GRA's Initial Operations Helped to Keep Qatar's Corruption-Induced World Cup Hosting Status Intact

141. On information and belief, Mr. Chalker's close relationship with the government of Qatar began before the formal "victory" of Qatar's bribe-laden bid[17] to host the World Cup in 2022.

142. In connection with that bid, Qatar has been credibly accused of bribery on a massive scale, offering to pay hundreds of millions of dollars to FIFA officials to secure hosting

[17] Rebecca R. Ruiz, *2 Top Soccer Officials Found Guilty in FIFA Case*, N.Y. Times (Dec. 22, 2017), https://www.nytimes.com/2017/12/22/sports/soccer/fifa-trial.html.

privileges.[18] A key force behind the corrupt bid—and holding onto it thereafter—was BlueFort /Spark Digital's Ahmad Nimeh (GRA code name "Botany").[19] Mr. Nimeh was a close contact of GRA's, and he was reportedly behind the "black ops" utilized to undermine the candidacy of Qatar's competitors seeking to host the 2022 World Cup—including the eventual runner-up, the United States.[20] (As discussed, BlueFort would later pay at least $3.9 million to Stonington Strategies, a ringleader in disseminating Mr. Broidy's hacked emails, shortly before the hacking campaign began.)

143. Qatar's corrupt bid eventually led to the convictions or guilty pleas of over sixteen individuals,[21] and the criminal investigation is not yet over—a superseding indictment outlining additional bribery charges was filed as recently as April 2020.[22]

144. At the time, and during the years that followed, Qatar's successful bid was met with enormous controversy, highlighting its precarious standing in the worldwide soccer community—a community that had never before voted to allow a Middle Eastern nation to host

---

[18] Alon Einhorn, *Qatar Offered FIFA $880 Million For Hosting the 2022 World Cup—Report*, The Jerusalem Post (Mar. 10, 2019), https://www.jpost.com/Middle-East/Qatar-offered-FIFA-880-million-for-hosting-the-2022-World-Cup-582998.

[19] Dan Friedman, *Qatari Lobbyists Received Millions Through Shadow Firm, Mother Jones* (Jan. 8, 2019), https://www.motherjones.com/politics/2019/01/qatari-lobbyists-received-millions-through-shadow-firm/

[20] *Id.*

[21] Press Release, U.S. Dep't of Justice, *Sixteen Additional FIFA Officials Indicted for Racketeering Conspiracy and Corruption* (Dec. 3, 2015), https://www.justice.gov/opa/pr/sixteen-additional-fifa-officials-indicted-racketeering-conspiracy-and-corruption.

[22] *See United States v. Webb, et al.*, No. 1:15-CR-00252 (E.D.N.Y.) (Apr. 6, 2020 Superseding Indictment).

its premier event.[23] Holding on to the 2022 World Cup—and the tremendous economic and reputational boost that goes along with it—was a matter of desperate national urgency.

145. On information and belief, starting around one year *prior* to the June 2013 handover of power from the previous Emir, Hamad Al Thani, to his fourth son, now-Emir Tamim bin Hamad Al Thani, the GRA Defendants focused more heavily on hacking and physical and electronic surveillance.

146. On information and belief, this shift to a more aggressive approach was at least in part driven to protect the now-Emir during his ascension to power. On information and belief, within months of the now-Emir replacing his father in June 2013, the GRA Defendants successfully proposed to Qatar a multi-year, global campaign based in significant part on "penetration" operations involving "black hat" hackers and other operators, with a requested total price tag of hundreds of millions of dollars. In the years since, the GRA Defendants have engaged in increasingly intrusive and illegal behavior to spy on Qatar's perceived enemies, including those seen as potential threats to the wealthy regime's interests.

147. Mr. Chalker and GRA actively pitched Qatar by offering Qatar access to some of the most highly trained former counterintelligence personnel in the world—to help secure Qatar's status as host. As controversy swirled in subsequent years, the GRA Defendants outlined their ability to employ intelligence community skills and covert action campaigns to neutralize key voices in the growing choir of critics who advocated that World Cup 2022 be reassigned to a different host country.

[23] *See FIFA World Cup Qatar 2022*, https://www.fifa.com/worldcup/destination/host-country/

148. In August 2012, a formal inquiry was launched to investigate Qatar's corrupt winning bid two years earlier by the International Federation of Association Football ("FIFA"), which is the global body governing competitive soccer, including the World Cup. On information and belief, the GRA Defendants shortly thereafter successfully convinced Qatar to fund an operation to use hacking and surveillance targeting FIFA executive committee members and related parties to gain "predictive intelligence" and "total information awareness." On information and belief, the real goal of obtaining "total information awareness"—relating to both professional communications and deeply private information—was not simply to intercept discussions of FIFA officials and investigators, but also to acquire blackmail- and extortion-type information that could be used to silence targeted individuals.

149. The investigation FIFA launched in 2012 documented extensive corruption, including bribery and astroturfing, utilized by Qatar to win the 2010 bid for the 2022 World Cup, and it was detailed in a 353-page report, known publicly as the "Garcia Report," based on the name of the lead investigator, former U.S. Attorney Michael J. Garcia. Even though the Garcia Report was submitted to FIFA in or around November 2014, it was not released to the public until a German news outlet in June 2017 published a leaked copy of the PDF of the full report. On information and belief, Defendants' campaign to hack and surveil FIFA officials targeted numerous executives and investigators connected to the Garcia Report, including FIFA's then-Secretary General Jérôme Valcke.

150. Ultimately, Qatar hired Mr. Chalker and GRA to conduct multiple operations, including "Project Riverbed," a covert campaign designed to target some of Qatar's biggest detractors, including Theo Zwanziger, the former president of the German Football Association and a then-current member of FIFA's executive committee. At the time, Mr. Zwanziger actively

promoted the idea of taking back Qatar's successful hosting bid and giving it to a different country. He referred to Qatar as "a cancer on world football"[24] and said that awarding the World Cup to Qatar was a "blatant mistake."[25] Project Riverbed's primary objective was to neutralize Mr. Zwanziger, by targeting him and influencing people close to him through covert influence and operations. The assignment included infiltrating FIFA itself.

151. In connection with Project Riverbed, Mr. Chalker and GRA's tactics included a covert action program, so-called "black ops," and the use of IT platforms. They targeted individuals and entities across multiple continents, set up and terminated multiple "cover for action" entities in various jurisdictions, and divided the administration of its work between "white" and "black" offices. (On information and belief, the division between white and black offices reflected legal and illegal work, so as to limit the number of people aware of the more sensitive or illicit operations.) GRA LLC (and by extension, Mr. Chalker) earned tens of millions of dollars for this work.

152. By the spring of 2014, Mr. Chalker and GRA had succeeded—Mr. Zwanziger had come full circle, and his public statements now generally supported World Cup 2022 remaining in Qatar as a way to improve social justice reform efforts there.

2. GRA Proposed Expanding Its Qatari Operations to Include Geopolitical Targets

153. On the heels of that success, in or around 2014, Mr. Chalker and GRA pitched Qatar for substantial additional work across multiple areas.

---

[24] *Former German FA president free to call Qatar 'a cancer on world football'*, The Guardian (Apr. 18, 2016).

[25] Kelyn Soong, *Awarding 2022 World Cup to Qatar was a 'blatant mistake,' FIFA member says,* Washington Post (July 24, 2013).

154. The proposed objective of one operation was to neutralize an expanded universe of perceived threats to Qatar's hosting status that were posed by members of the FIFA Executive Committee; individual FIFA confederations and nations; the most significant corporate sponsors; European domestic leagues; and individual political leaders within the worldwide soccer community.

155. Another operation was an even broader effort aimed at identifying in real time additional threats to Qatar's World Cup bid, even before those threats became public. A related campaign, referred to as Operation Frosty, was aimed specifically at monitoring officials with the Asian Football Confederation, whose territory includes the Gulf region and GCC nations.

156. For these projects, GRA allocated up to ten dedicated "black hat" operatives for covert operations such as hacking, with the goal of providing Qatar with advanced warning of any shifting opinions on Qatar's bid. GRA's promises of advanced warnings were premised on its ability to conduct unlawful hacking and other illegal surveillance. GRA informed its primary client that its operations would allow Qatar to neutralize threats to the World Cup while maintaining deniability and avoiding retaliation or punishment should the illegal conduct be discovered.

157. GRA's requested price tag for this work exceeded $500 million, which would be a relatively modest sum for the world's wealthiest per-capita nation because the controversy surrounding Qatar's hosting status had exploded, and Qatar's hosting privileges were in in peril. For example, a widely-covered report by Amnesty International documented slave-like labor conditions in Qatar's construction sector where workers went without pay for months on end (or

sometimes without pay at all), had their passports confiscated so they could not leave the country, and were forced to live in "squalid" accommodations.[26]

158. Mr. Chalker and GRA again pushed a covert action campaign to mitigate these damaging allegations that threatened to derail Qatar's hosting opportunity. They motivated Qatar by warning that the time for half-measures was over. Instead, they advocated persistent and aggressive distractions and disruptions to put Qatar's attackers on the defensive.

159. Mr. Chalker and GRA also sought expanded opportunities to assist Qatar on a broader geopolitical front. Despite being a petroleum-rich nation with substantial financial resources, Qatar lacked high-end technological capabilities. Mr. Chalker and GRA identified and proposed multiple national security enhancements and surveillance work, including "Project Deviant," in which GRA would train Qatari officers in defensive counter-intelligence and offensive intelligence collection tactics, including advanced, sophisticated skills that trained former U.S. intelligence and military operatives are typically barred from sharing or conferring unto foreign governments.

160. In promoting a global strategic plan, Mr. Chalker and GRA convinced Qatar to go on the offensive, by bolstering a Washington, DC-based lobbying campaign and leveraging technology partners to harness massive volumes of data. And they stressed that outsourcing this effort to Mr. Chalker and GRA would enable Qatar to maintain full deniability and avoid retaliation from sophisticated enemies. GRA's efforts to silence and neutralize Mr. Broidy—through aggressive cyberattacks and collaboration with media professionals to disseminate the spoils—reflect this strategy.

---

[26] Amnesty International, *The Dark Side of Migration: Spotlight on Qatar's Construction Sector Ahead of the World Cup* (Nov. 18, 2013), https://www.amnesty.org/download/Documents/16000/mde220102013en.pdf

B. GRA's Attack on Mr. Broidy and BCM Coincided with the Expansion of Its Work for the Qatari-Funded Criminal Enterprise

1. Qatar Became GRA's Most Important Client

161. As outlined by GRA itself, and consistent with its unique areas of expertise, GRA was retained in part to target Qatar's political enemies through cyber operations and public relations, to protect Qatar's geopolitical interests. On information and belief, Qatar retained GRA to execute these larger-scale programs on its behalf and entered into consultancy arrangements with GRA worth at least $100 million, primarily for covert and typically illegal conduct.

162. Throughout this time, Mr. Chalker's relationship with key members of Qatar's leadership grew stronger—the same Qatari leaders with whom the PR strategists who disseminated Plaintiffs' stolen documents to the media also worked closely. As noted above, GRA had code names for several of them: "Apex" (the Emir); "Mightier" (the Emir's brother, MBH); and "Shep" (MBH's chief of staff, al Thawadi).

163. Mr. Chalker maintained particularly close contact with Shep. GRA's U.S.-based teams would regularly compile and synthesize the results of their covert intelligence gathering, including their hacking and physical and electronic surveillance efforts, and produce a glossy, printed deliverable for Shep every two to three months. The information GRA brought to Shep included highly personal, non-public information on American citizens.

164. Spying on Americans was part of what GRA referred to as "special projects." GRA compartmentalized its "special projects" because it well knew that the special projects involved extensive criminal conduct. Another initiative falling within "special projects" was the effort to denigrate UAE's ambassador to the United States, including the hacking of his emails (discussed below) and surveillance of him, as well as those who interacted with him, including

Americans. The invoices and other records of these projects were kept separate from GRA's above-board work for Qatar.

165. On information and belief, Defendant Kevin Chalker used various U.S. and offshore companies, such as Technical Data Analytics Limited of Bermuda, TechPro Maritime Solutions LLC, Bernoulli Limited and Toccum Limited, primarily or exclusively for paying "off-books" operatives who performed unethical or even illegal actions, including Special Forces soldiers and U.S. government employees who serve in the intelligence community and law enforcement.

166. GRA's "off-books" operations for Qatar were highly lucrative. As of December 2017, during the time leading up to the attack on Mr. Broidy and BCM, Mr. Chalker held over $40 million in cash in accounts affiliated with Bernoulli Limited and Toccum Limited, shell companies formed in Gibraltar and for which he served as the sole director. And on information and belief, in or around 2017 and 2018, the overwhelming majority of GRA's revenue—and almost all of its overseas revenue—came from Qatar-related work, mostly for illegitimate and illegal work product.

167. On information and belief, Global Risk Advisors EMEA Limited—the contracted GRA entity that performed the "official" work for Qatar—showed less than $2 million in revenue in its unaudited financial statements. The 2017 balance sheet that EMEA Limited submitted to Gibraltar authorities showed a slightly larger increase in year-over-year cash on hand, increasing from a paltry USD $33.00 to just under $3.3 million. Thus, the self-reported financial disclosures indicate that Mr. Chalker's companies set up to receive payments for and fund illicit activities took in at least ten times the amount paid to the GRA entity that performed the legitimate, "official" work for GRA's primary client.

168. Reflecting their close relationship, GRA expanded its partnership with Qatar. In or around mid-August 2017, Qatar and GRA reached an agreement on a broad cybersecurity and surveillance arrangement, approved by Hassan Al Thawadi ("Archie"), who is Shep's brother and the Secretary General of the Supreme Committee for Delivery and Legacy. On information and belief, the agreement called for GRA to work directly with Qatar's Special Forces and intelligence collection agencies, including on cybersecurity, surveillance, and countersurveillance.

169. On or around the time when the broad cybersecurity and surveillance agreement was reached, GRA offered a proposal to Qatar that contained some of the same coded phrases used by GRA going back to at least 2012-2013, such as utilizing "Enhanced Early- Warning Systems" to achieve "Global Influence" and to "Dominate GCC Geopolitical Issues."

170. On information and belief, during the negotiation and implementation of GRA's broad cybersecurity and surveillance agreement with Qatar, GRA relied upon the advice and feedback of a supposedly former employee who at that time in the summer and fall of 2017 worked in the West Wing of the White House.

171. Within days of reaching agreement on the cybersecurity and surveillance arrangement with Qatar, Messrs. Chalker and Mandich incorporated in Delaware a new cybersecurity company, Defendant Qrypt Inc., on or around August 24, 2017.

172. GRA soon expanded its physical presence in Qatar. In October 2017, during the planning stages of the upcoming attack on Mr. Broidy, GRA registered Global Risk Advisors (EMEA) Limited (Qatar Financial Centre Branch), a branch of Gibraltar-incorporated Global Risk Advisors EMEA Limited, in Doha, Qatar. The Doha branch was de-registered on February

19, 2020. Eleven months before the branch was de-registered, though, GRA EMEA LLC was created in the Qatar Financial Centre in Doha on March 19, 2020.

173. On information and belief, Mr. Chalker in 2019 assigned a 70% ownership stake of GRA EMEA LLC and at least five of his Gibraltar companies and at least one in Luxembourg to the Chalker Family Trust of 2018, whose sole ultimate beneficial owners are his two teenage sons, and 30% to his brother, Defendant Courtney Chalker.

2. GRA Conducted Multiple Similar Cyberattacks for the Qatari-Funded Criminal Enterprise

174. Mr. Broidy was not the only cyberattack target.[27] GRA's covert cyber operations involved a pattern of attacks against political targets involving similar fake news alerts, malicious Google login pages, email addresses designed to mimic legitimate Google security addresses, falsified two-factor authentication messages, and the use of Mail.ru to control victims' accounts.

175. As has been publicly reported in *The New York Times* and other media outlets, forensic evidence indicates that Qatar, and therefore GRA, were likely involved in targeting over 1,000 people and entities via cyberattacks similar to those deployed against Plaintiffs here, including prominent officials from countries like Egypt and the UAE, and the United States, including an American political columnist and activist, Rabbi Shmuley Boteach, all of whom are known as outspoken critics of Qatar.[28]

---

[27] *See* Eli Lake, *Russian Hackers Aren't the Only Ones to Worry About*, Bloomberg (Sept 18, 2018), https://www.bloomberg.com/opinion/articles/2018-09-18/russian-hackers-aren-t-the-only-ones-to-worry-about.

[28] *See* Shmuley Boteach, "Qatar's War to Destroy Pro-Israel Jews," Jerusalem Post, Oct. 8, 2018, https://www.jpost.com/Opinion/Qatars-war-to-destroy-pro-Israel-Jews-568942; Eli Lake, "Russian Hackers Aren't the Only Ones to Worry About," Bloomberg, Sept. 18, 2018,

176. One of the targeting projects was highly successful and has particular salience here: GRA's hacking and surveillance of the UAE Ambassador to the United States. In or around April and May 2017, approximately a half-year before it attacked Mr. Broidy, GRA conducted similar cyberattacks against the UAE Ambassador, who has extensive interactions with politically active Americans, in an effort to improve Qatar's image with the United States by not only discrediting him, but also intimidating (and ultimately silencing) U.S. government officials who were either critics or potential critics of Qatar.

177. As with Mr. Broidy, hacked emails were disseminated to the media by an anonymous "source" identified only by an alias— "Global Leaks"—in an effort to embarrass not just the primary target, but also politically active associates, ultimately silencing active critics and preventing others from voicing their own criticisms.

178. On information and belief, Defendant Mandich was the mastermind who architected the Global Leaks operation, overseeing the execution of every phase of the operation. On information and belief, John Sabin and Defendants Garcia and Kevin Chalker also worked with Mr. Mandich in carrying out the Global Leaks campaign. On information and belief, Mr. Chalker began paying Mr. Madich "off-books" in 2016, starting at least six months before the latter's official retirement from the CIA in 2017.

179. In June 2017, *The Huffington Post* wrote one of the first stories under the headline "Someone Is Using These Leaked Emails To Embarrass Washington's Most Powerful Ambassador."[29] The article stated that, "In private correspondence, [UAE Ambassador]

---

https://www.bloomberg.com/opinion/articles/2018-09-18/russian-hackers-aren-t-the-only-onesto-worry-about.

[29] Akbar Shahid Ahmed, *Someone Is Using These Leaked Emails To Embarrass Washington's Most Powerful Ambassador*, The Huffington Post (June 3, 2017).

Otaiba—an extremely powerful figure in Washington, D.C., who is reportedly in 'in almost constant phone and email contact' with Jared Kushner, President Donald Trump's adviser and son-in-law—is seen pushing for the U.S. to close down its military base in Qatar and otherwise poking at issues that could drive a wedge between the U.S. and that Arab nation."

180. Another article, published in *The Intercept*, was titled "Diplomatic Underground: The Sordid Double Life of Washington's Most Powerful Ambassador," and was clearly designed to embarrass the UAE Ambassador.[30] The article relied on hacked emails, and notes that the emails "began to dribble out just as a geopolitical row between the UAE and its neighbors in Qatar came to a head."

181. An article in *The New York Times*, based on hacked emails, was likewise intended to embarrass the UAE, this time by showing that the UAE had at one point tried to get the Taliban to open an embassy there.[31] The article states: "Anonymous hackers have provided a long series of leaked emails from Ambassador Yousef al-Otaiba's Hotmail account to *The New York Times* and other news organizations over the past two years in an apparent campaign to embarrass the U.A.E. and benefit Qatar."

182. There are striking similarities to the attack on Elliott Broidy. Both attacks were disseminated to some of the same friendly reporters, including Ryan Grim (*The Intercept*), Bradley Hope (*The Wall Street Journal*), and David Kirkpatrick (*The New York Times*). Upon information and belief, Mr. Howard was among the public relations professionals pitching stories based on the hacked material, just as he would later do with the Broidy hack. And the execution

[30] Ryan Grim, Diplomatic Underground: The Sordid Double Life of Washington's Most Powerful Ambassador, *The Intercept* (Aug. 30, 2017).

[31] David D. Kirkpatrick, *Persian Gulf Rivals Competed to Host Taliban, Leaked Emails Show*, N.Y. Times (July 31, 2017).

of the two attacks included several tactics in common, such as: (1) use of messages from Gmail accounts that appeared to be official; (2) messages that displayed a correct but redacted phone number for the victim; (3) deployment of evasion tactics to help bypass automatic spam filter and other security alerts; (4) use of private registration services and "throw away accounts" from the Mail.Ru group; and (5) maintenance of multiple phishing sites but hosting them on their own dedicated servers, using different subdomains for different campaigns. GRA swiftly took down sites that appeared to have been noticed, redirecting them all to the www.accessdenied.com site (HTTP 302 code). On information and belief, the UAE Ambassador relied on GRA's fraudulent misrepresentations and unwittingly provided his confidential login credentials, thus enabling GRA to hack him.

183. Indeed, the similarities were lost on no one. The BBC quoted an unnamed "source familiar" with the hack as saying that the Broidy attack was "rinse and repeat on Otaiba."[32]

184. Moreover, the UAE Ambassador hack was successful in silencing certain critics of Qatar. For example, the Foundation for the Defense of Democracies (FDD) had consistently criticized Qatar's support for Islamic extremism and terrorism. On May 23, 2017, FDD hosted (with Plaintiffs' involvement) a conference largely focused on exposing Qatar's misdeeds. Less than a week later, after learning that their communications had been intercepted in the UAE Ambassador hack, FDD executive director Mark Dubowitz informed Mr. Broidy that the think tank would no longer publicly criticize the wealthy emirate because they feared potential Qatari reprisal. Two months later, the only FDD scholar whose work had substantially focused on

[32] Suzanne Kianpour, Emails show UAE-linked effort against Tillerson (Mar. 5, 2018), https://www.bbc.com/news/world-us-canada-43281519

Qatar left the think tank, and no one was hired or reassigned to replace his work relating to Qatar.

185. GRA's numerous cyberattacks have extended over several years and represent a pattern of unlawfully accessing victims' computer systems to extract private information or other items of value with which to attack or damage the enemies of its clients.

186. In addition to cyberattacks in which information was stolen, Qatar has used unlawful and unauthorized access to computer systems to plant documents that would appear to incriminate their purported enemies.

187. These cyberattacks are all part of the pattern of racketeering activity in which the Enterprise conspirators have engaged with the common purpose of silencing critics of Qatar.

III. PLAINTIFFS FILED LAWSUITS AGAINST INDIVIDUAL MEMBERS OF THE QATARI-FUNDED CRIMINAL ENTERPRISE

188. On March 19, 2018, Mr. Broidy and BCM, through counsel, formally requested that Qatar take appropriate action to halt the attacks on Plaintiffs' emails, documents, and data, to stop the GRA Defendants from disseminating Plaintiffs' emails, documents, and data, and/or to assist Plaintiffs in halting their dissemination, if the hack had been conducted by a rogue agent of Qatar.

189. When Qatar failed to respond to Plaintiffs' request, Mr. Broidy and BCM filed suit in the United States District Court for the Central District of California against Qatar, certain of the GRA Defendants here, and several other individuals and entities responsible for the hacking scheme on March 26, 2018. On May 4, 2018, the parties stipulated to a stay to permit limited discovery. In conducting this discovery, Plaintiffs were able to uncover the phone records for some of the co-conspirators and others, as well as some WhatsApp chats among Mr. Muzin, Mr. Allaham, and other conspirators. Plaintiffs used this narrow opportunity for

discovery to substantiate the above allegations. However, this discovery was limited to establishing jurisdiction in that case, and did not reach the merits of any of Plaintiffs' claims. In addition, a large portion of the discovery was marked "Confidential" under the governing protective order, prohibiting the Plaintiffs from using it to further substantiate the allegations above.

190. The lawsuit triggered a panic within GRA, which was eager to destroy the evidence inculpating it in the hacking scheme. Kevin Chalker instructed GRA's Chief Security Officers, also a GRA Research hacker in the Reston Group, Anthony Garcia, to wipe GRA's computers, phones and other devices clean of any damaging evidence. Mr. Garcia not only complied with that instruction, but he removed certain hard drives, phones and devices with incriminating evidence from GRA's offices, and brought them to a remote location, where the devices were destroyed and ultimately discarded. Upon information and belief, Defendant Courtney Chalker knowingly assisted Mr. Garcia with the destruction of evidence.

191. The district court dismissed the lawsuit against Qatar on grounds of foreign sovereign immunity, and dismissed all other served defendants for lack of personal jurisdiction. The court did not reach the merits of any claims, and its decision dismissing Qatar is currently under appeal.

192. On July 23, 2018, Plaintiffs also filed suit in the United States District Court for the Southern District of New York against Jamal Benomar. The district court dismissed the case without permitting any jurisdictional discovery, on grounds of diplomatic immunity. The Second Circuit affirmed that decision. Neither the district court nor the Second Circuit reached the merits of any of Plaintiffs' claims.

193. On January 24, 2019, Plaintiffs filed suit against Nicholas Muzin, Joseph Allaham, Gregory Howard, and Stonington Strategies. *See Broidy Capital Mgmt. v. Muzin et al.*, No. 19-cv-00150 (D.D.C. filed Jan. 24, 2019) (Friedrich, J.). After briefing and argument on a motion to dismiss, on March 31, 2020, Judge Freidrich largely upheld the operative complaint. 2020 WL 1536350 (D.D.C. Mar. 31 2020).

194. On December 27, 2019, Plaintiffs filed this suit. Plaintiffs sued in this Court, and not in the District of Columbia, to ensure that there would be personal jurisdiction over GRA. Defendant GRA LLC (the parent entity of all other GRA-related Defendants) is headquartered in this District, and Kevin Chalker—the ultimate owner of GRA LLC and all other GRA-related entities and the mastermind of the hacking scheme—lives in this District. Plaintiffs' first suit against GRA was dismissed because the court in California concluded that GRA lacked sufficient contacts with California. While Plaintiffs disagreed with that ruling, it was not worth taking the risk of having the same result occur in the District of Columbia, and thereby having to file a third suit. That would not only be a huge waste of time, but it would present the needless risk of creating statute of limitations defenses that otherwise would not exist.

CAUSES OF ACTION

COUNT ONE

(Against all GRA Defendants)

Stored Communications Act
18 U.S.C. § 2701 *et seq.*

195. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this First Amended Complaint.

196. The Stored Communications Act imposes criminal penalties on "whoever . . . intentionally accesses without authorization a facility through which an electronic

communication service is provided. . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system . . . ." 18 U.S.C. § 2701(a).

197. The Act also provides that "a person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity" damages, along with equitable and declaratory relief. *Id.* § 2707.

198. Plaintiffs are "persons" within the meaning of 18 U.S.C. §§ 2510(6) and 2707(a).

199. The GRA Defendants are directly liable under the SCA for conducting and supervising the hacking of Plaintiffs' email servers and computer systems.

200. The GRA Defendants willfully and intentionally accessed without authorization a facility through which an electronic communication service is provided, namely, BCM's computer systems, including its email servers, as well as Google's servers, thereby obtaining access to wire or electronic communications while they were in electronic storage in such systems, in violation of 18 U.S.C. § 2701(a).

201. The cyberattack was a willful, flagrant, and intentional violation of the Stored Communications Act.

202. The GRA Defendants willfully and intentionally accessed the email accounts of, at least, Robin Rosenzweig and Mr. Broidy's Executive Assistant, by transmitting fake spear phishing emails with links to malicious websites enabling Defendants to steal their login credentials.

203. Thereafter, the GRA Defendants used the information they obtained from their spear phishing attacks to gain unauthorized access to Plaintiffs' computer networks and email

accounts. Beginning on or about January 16, 2018, the GRA Defendants intentionally accessed or caused to be accessed BCM's servers without authorization, including emails and documents physically located on those servers, as well as Google servers, specifically by accessing, or causing others to access, the accounts of Mr. Broidy and other BCM employees, without authorization.

204. The GRA Defendants also implemented identifiable obfuscation techniques, such as VPN, to engage in efforts to hide the origin of their spear phishing attacks and unauthorized access to Plaintiffs' servers, and emails and documents physically located on those servers and the servers of Google. The GRA Defendants used VPN and other tools to mask their cyber intrusions and avoid detection, thereby showing sophistication and consciousness of guilt.

205. The GRA Defendants intentionally, willfully, unlawfully, and without authorization accessed Plaintiffs' computer systems and email servers thousands of times over a period of almost two months, in a sustained cyberattack.

206. As a direct and proximate result of the actions of the GRA Defendants, Plaintiffs incurred substantial losses and damage, including but not limited to:

(a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;

(b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

(c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;

(d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Mr. Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill; and

(e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation.

207. The GRA Defendants intentionally and willfully caused such damage to Plaintiffs.

208. As provided for in 18 U.S.C. § 2707(b) & (c), Plaintiffs are entitled to an award of the greater of the actual damages suffered or the statutory damages, as well as punitive damages, attorneys' fees and other costs of this action, and appropriate equitable relief.

209. The GRA Defendants' conduct has caused, and will continue to cause, Plaintiffs irreparable injury, including loss of goodwill, an increased risk of further theft, and an increased risk of harassment. Plaintiffs have been forced to expend considerable time, money and effort

safeguarding their personal information in the wake of these series of hacks. Plaintiffs will continue to suffer this injury as long as their personal information is available to Defendants, and subsequently, to media organizations and the world at large. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting Defendants from engaging in any further cyberattacks or in the conduct described in this Cause of Action.

COUNT TWO

(Against all GRA Defendants)

Computer Fraud and Abuse Act
18 U.S.C. § 1030(a)(2) and (a)(5)

210. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this First Amended Complaint.

211. The Computer Fraud and Abuse Act creates a cause of action against whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2).

212. The Act also creates a cause of action against whoever "(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss." *Id.* § 1030(a)(5).

213. The Act also creates a cause of action against "[w]hoever conspires to commit or attempts to commit an offense under subsection (a) of this section." *Id.* § 1030(b).

214. A "protected computer" is one that "is used in or affecting interstate or foreign commerce or communication." *Id.* § 1030(e)(2)(B).

215. BCM's computer systems and email servers are used in and affect interstate and foreign commerce or communication and are therefore "protected computers."

216. The GRA Defendants willfully and intentionally accessed the email accounts of, at least, Robin Rosenzweig and Mr. Broidy's Executive Assistant, by transmitting fake spear phishing emails with links to malicious websites enabling Defendants to steal their login credentials.

217. Thereafter, the GRA Defendants used the information they obtained from their spear phishing attacks to gain unauthorized access to Plaintiffs' computer networks and email accounts. Beginning on or about January 16, 2018, the GRA Defendants intentionally accessed or caused to be accessed BCM's servers without authorization, including emails and documents physically located on those servers, as well as Google servers, specifically by accessing, or causing others to access, the accounts of Mr. Broidy and other BCM employees, without authorization.

218. The GRA Defendants also implemented identifiable obfuscation techniques, such as VPN, to engage in efforts to hide the origin of their spear phishing attacks and unauthorized access to Plaintiffs' servers, and emails and documents physically located on those servers and the servers of Google. The GRA Defendants used VPN and other tools to mask their cyber intrusions and avoid detection, thereby showing sophistication and consciousness of guilt.

219. The GRA Defendants intentionally, willfully, unlawfully, and without authorization accessed Plaintiffs' protected computer systems and email servers thousands of

times over a period of almost two months, in a sustained cyberattack. The GRA Defendants intentionally conspired to cause damage to BCM's protected computers through the attack.

220. They knowingly caused the transmission of a program, information, code, or command, and as a result, intentionally caused damage without authorization, to BCM's protected computers.

221. As a direct and proximate result of the actions of the GRA Defendants, Plaintiffs incurred substantial losses and damage, including but not limited to:

(a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;

(b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

(c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;

(d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Mr. Broidy's and other employees' time spent investigating the hacking, taking remedial measures in

response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill; and

(e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation.

222. The total amount of these losses will be proven at trial but, in any event, far exceeds $75,000. In fact, the out-of-pocket costs Plaintiffs paid to outside consultants to conduct a damage assessment and for remedial measures was alone in the hundreds of thousands of dollars.

223. The GRA Defendants intentionally and willfully caused such damage to Plaintiffs.

224. The GRA Defendants' conduct has caused, and will continue to cause, Plaintiffs irreparable injury, including loss of goodwill, an increased risk of further theft, and an increased risk of harassment. Plaintiffs have been forced to expend considerable time, money and effort safeguarding their personal information in the wake of these series of hacks. Plaintiffs will continue to suffer this injury as long as their personal information is available to Defendants, and subsequently, to media organizations and the world at large.

COUNT THREE

(Against all GRA Defendants)

Misappropriation of Trade Secrets
(18 U.S.C. §§ 1831, 1832, 1836)

225. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this First Amended Complaint.

226. Federal law creates a cause of action against "[w]hoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret, knowingly . . . steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains" trade secrets. 18 U.S.C. § 1832(a)(1).

227. Federal law imposes criminal penalties on "whoever . . . conspires with one or more other persons" to violate § 1832(a)(1). *See id.* § 1832(a)(5).

228. Federal law also creates a cause of action against "[w]hoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret." *Id.* § 1831(a)(1).

229. Federal law imposes penalties on "[w]hoever . . . conspires with one or more other persons to commit" the offense listed in § 1831(a)(1). *See id.* § 1831(a)(5).

230. "An owner of a trade secret that is misappropriated may bring a civil action. . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." *Id.* § 1836(b)(1). The owner may seek remedies including, *inter alia*, injunctive relief and "damages for actual loss caused by the misappropriation of the trade secret." *Id.* § 1836(b)(3)(A-B).

231. The BCM computer systems and email servers stored trade secrets, including but not limited to highly confidential business plans and proposals; research supporting those plans and proposals, including cost proposals and service projections; information concerning business

strategies and opportunities; and contacts for important business relationships. These trade secrets are of substantial value to Plaintiffs, as will be proven at trial.

232. BCM stored trade secrets that were used in interstate and foreign commerce.

233. Plaintiffs have taken and continue to take reasonable measures to maintain the secrecy of their trade secrets. For example, Plaintiffs have always maintained their information on secured servers that are protected by passwords, firewalls, and antivirus software.

234. Moreover, Plaintiffs' emails contained confidential information involving contracts, business proposals, and cost estimates involving Mr. Broidy's company and its clients. These contracts, proposals, and estimates contained sensitive information about Mr. Broidy's clients and his company's confidential technology and methods.

235. Plaintiffs' trade secrets derive independent actual and potential economic value from not being generally known or available to the public or other persons who can obtain economic value from their disclosure or use.

236. Plaintiffs' trade secrets have significant value, resulting from significant investment of time and resources.

237. The GRA Defendants unlawfully conspired to take, appropriate, and obtain Plaintiffs' trade secrets without authorization, by means of a cyberattack against Plaintiffs. Defendants knew that BCM's servers contained trade secrets and intended to steal them in order to harm Plaintiffs.

238. The GRA Defendants directly misappropriated Plaintiffs' trade secrets during the hacking of their computer systems and email servers. These trade secrets included confidential business plans, stored on plaintiffs' servers, cost proposals and service projections, information

concerning business strategies and opportunities, and contacts for important business relationships.

239. The GRA Defendants improperly disclosed and misappropriated Plaintiffs' trade secrets without consent or authorization when they widely disseminated those trade secrets to fellow members of the Qatari-Funded Criminal Enterprise, who then distributed them to the media. At the time of such disclosures, the GRA Defendants knew or had reason to know that the information disclosed consisted of trade secrets.

240. The GRA Defendants misappropriated Plaintiffs' trade secrets intentionally for the benefit their foreign client, Qatar, as well as the Qatari-Funded Criminal Enterprise, and acted with the knowledge that their actions would have the effect of benefiting both the foreign government of Qatar as well as the Enterprise.

241. The GRA Defendants' acts of misappropriation have affected interstate commerce.

242. As a direct and proximate result of the actions of the GRA Defendants, Plaintiffs incurred substantial losses and damage, including but not limited to:

(a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;

(b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

(c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;

(d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Mr. Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill; and

(e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation.

243. The total amount of these losses will be proven at trial but, in any event, far exceeds $75,000. In fact, the out-of-pocket costs Plaintiffs paid to outside consultants to conduct a damage assessment and for remedial measures was alone in the hundreds of thousands of dollars. *See* 18 U.S.C. § 1836(b)(3)(B)(i)(I).

244. As a direct consequence of Defendants' unlawful actions, the GRA Defendants have unjustly benefited from their possession of Plaintiffs' trade secrets. The GRA Defendants were paid money by the Qatari-Funded Criminal Enterprise to conspire to misappropriate Plaintiffs' trade secrets. Plaintiffs seek damages in the amount of that unjust enrichment, and disgorgement of the GRA Defendants' profits pursuant to 18 U.S.C. § 1836(b)(3)(B)(i)(II).

245. The GRA Defendants' conduct was willful and malicious, and thus Plaintiffs are entitled to exemplary damages pursuant to 18 U.S.C. § 1836(b)(3)(C), equal to twice the amount of their proven damages. Plaintiffs are also entitled to attorneys' fees pursuant to 18 U.S.C. § 1836(b)(3)(C).

246. The GRA Defendants' conduct has caused, and will continue to cause, Plaintiffs irreparable injury, including loss of goodwill, an increased risk of further theft, and an increased risk of harassment. Plaintiffs have been forced to expend considerable time, money and effort safeguarding their personal information in the wake of these series of hacks. Plaintiffs will continue to suffer this injury as long as their personal information is available to the GRA Defendants, and subsequently, to media organizations and the world at large. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting the GRA Defendants from misappropriating its trade secrets or engaging in any other conduct described in this Cause of Action.

247. The GRA Defendants' conduct constitutes criminal conduct in violation of 18 U.S.C. §§ 1831 and 1832. As such, it constitutes predicate racketeering activity under the Racketeer Influenced and Corrupt Organizations ("RICO") Act, 18 U.S.C. § 1962.

COUNT FOUR

(Against all GRA Defendants)

Misappropriation of Trade Secrets
Uniform Trade Secrets Act
Cal. Civ. Code § 3426 *et seq.*

248. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this First Amended Complaint.

249. The law of the State of California provides a cause of action for damages and injunctive relief in response to the misappropriation of trade secrets. Cal. Civ. Code §§ 3426.2;

3426.3. (While Plaintiffs believe this claim is governed by California law, in the alternative, Plaintiffs hereby allege, based on the same facts, that Defendants have committed misappropriation of trade secrets under New York common law.)

250. The GRA Defendants misappropriated a "trade secret" as defined by Cal. Civ. Code § 3426.1 to include "information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

251. The BCM server stored trade secrets, including but not limited to highly confidential business plans and proposals; research supporting those plans and proposals, including cost proposals and service projections; information concerning business strategies and opportunities; and contacts for important business relationships. These trade secrets are of substantial value to Plaintiffs, as will be proven at trial.

252. Moreover, Plaintiffs' emails contained confidential information involving contracts, business proposals, and cost estimates involving Mr. Broidy's company and its clients. These contracts, proposals, and estimates contained sensitive information about Mr. Broidy's clients and his company's confidential technology and methods.

253. Plaintiffs have taken and continue to take reasonable measures to maintain the secrecy of their trade secrets. For example, Plaintiffs have always maintained their information on secured servers that are protected by passwords, firewalls, and antivirus software.

254. Plaintiffs' trade secrets derive independent actual and potential economic value from not being generally known or available to the public or other persons who can obtain economic value from their disclosure or use.

255. Plaintiffs' trade secrets have significant value, resulting from significant investment of time and resources.

256. The GRA Defendants directly misappropriated Plaintiffs' trade secrets by committing and supervising a hack into BCM's computer systems and email servers.

257. The GRA Defendants improperly disclosed and misappropriated Plaintiffs' trade secrets without consent or authorization when they widely disseminated those trade secrets to fellow members of the Qatari-Funded Criminal Enterprise and to media organizations for publication. At the time of such disclosure, the GRA Defendants knew or had reason to know that the information disclosed consisted of trade secrets.

258. As a direct and proximate result of the actions of the GRA Defendants, Plaintiffs incurred substantial losses and damage, including but not limited to:

(a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;

(b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

(c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business

computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;

(d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Mr. Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill; and

(e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation.

259. The total amount of these losses will be proven at trial but, in any event, far exceeds $75,000.

260. As a direct consequence of the GRA Defendants' unlawful misappropriation of Plaintiffs' trade secrets, the GRA Defendants have unjustly profited from their possession of Plaintiffs' trade secrets. The GRA Defendants were paid money from the Qatari-Funded Criminal Enterprise to steal and misappropriate Plaintiffs' trade secrets. Plaintiffs seek damages in the amount of that unjust enrichment, and disgorgement of the GRA Defendants' profits.

261. The GRA Defendants' conduct was willful and malicious, and thus Plaintiffs are entitled to exemplary damages pursuant to Cal. Civ. Code § 3426.3, equal to twice the amount of their proven damages. Plaintiffs are also entitled to attorneys' fees pursuant to Cal. Civ. Code § 3426.4.

262. The GRA Defendants' conduct has caused, and will continue to cause, Plaintiffs irreparable injury, including loss of goodwill, an increased risk of further theft, and an increased risk of harassment. Plaintiffs have been forced to expend considerable time, money and effort safeguarding their personal information in the wake of these series of hacks. Plaintiffs will continue to suffer this injury as long as their personal information is available to the GRA Defendants, and subsequently, to media organizations and the world at large. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting the GRA Defendants from misappropriating its trade secrets or engaging in any other conduct described in this Cause of Action.

COUNT FIVE

(Against all GRA Defendants)

California Comprehensive Computer Data Access and Fraud Act
Cal. Pen. Code § 502

263. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this First Amended Complaint.

264. California law imposes criminal penalties on anyone who "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network. Cal. Pen. Code § 502(c)(2).

265. California law imposes criminal penalties on anyone who "[k]nowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network." *Id*. § 502(c)(4).

266. California law imposes criminal penalties on anyone who "[k]nowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of" Section 502. *Id*. § 502(c)(6).

267. California law imposes criminal penalties on anyone who "[k]nowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network. *Id.* § 502(c)(7).

268. California law imposes criminal penalties on anyone who "[k]nowingly and without permission uses the Internet domain name or profile of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages or posts and thereby damages or causes damage to a computer, computer data, computer system, or computer network." *Id.* § 502(c)(9).

269. California law provides that "the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access." *Id*. § 502(e)(1).

270. California law provides for award of reasonable attorneys' fees. *Id*. § 502(e)(2).

271. The GRA Defendants knowingly and unlawfully accessed computers, computer systems or computer networks at Plaintiff BCM and Google, all of which were located in California. The GRA Defendants knew that at the time that they did not have the authorization to access Plaintiffs' computers, computer systems, and networks. This knowledge is

demonstrated by conspirators' use of spear phishing attacks and attempted spear phishing attacks to disguise their intentions and obtain login credentials through fraudulent misrepresentations. The spear phishing emails imitated Google's profile in order to obtain login credentials. The GRA Defendants caused damage to Plaintiffs' electronic files and emails through their cyber intrusions.

272. The GRA Defendants knowingly and unlawfully conducted the hacking of BCM's computer systems and email servers, and are therefore directly liable under the Act.

273. As a direct and proximate result of the actions of the GRA Defendants, Plaintiffs incurred substantial losses and damage, including but not limited to:

(a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;

(b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

(c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;

(d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media

onslaught, losses associated with hundreds of hours of Mr. Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill; and

(e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation.

274. The total amount of these losses will be proven at trial but, in any event, far exceeds $75,000. In fact, the out-of-pocket costs Plaintiffs paid to outside consultants to conduct a damage assessment and for remedial measures was alone in the hundreds of thousands of dollars. These losses include significant costs that were reasonably necessary to verify whether and how Plaintiff's computer systems and data were altered, damaged or deleted by the GRA Defendants' unlawful access.

275. The GRA Defendants' actions were willful and malicious, and Plaintiffs are entitled to punitive damages under § 502(e)(4).

276. The GRA Defendants' actions have caused, and will continue to cause, Plaintiffs irreparable injury, including loss of goodwill, an increased risk of further theft, and an increased risk of harassment. Plaintiffs have been forced to expend considerable time, money and effort safeguarding their personal information in the wake of these series of hacks. Plaintiffs will continue to suffer this injury as long as their personal information is available to Defendants, and subsequently, to media organizations and the world at large. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction requiring the GRA Defendants to refrain from engaging in any conduct described in this Cause of Action.

COUNT SIX

(Against all GRA Defendants)

Receipt and Possession of Stolen Property in Violation of Cal. Pen. Code § 496

277. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this First Amended Complaint.

278. California law imposes criminal penalties on any "person who buys or receives any property that has been stolen or that has been obtained in any manner constituting theft or extortion, knowing the property to be so stolen or obtained, or who conceals, sells, withholds, or aids in concealing, selling or withholding any property from the owner, knowing the property to be so stolen or obtained." Calif. Penal Code § 496(a).

279. California law further provides that "[a]ny person who has been injured by a violation of [Section 496] may bring an action for three times the amount of actual damages, if any, sustained by plaintiff, costs of suit, and reasonable attorney's fees."

280. The GRA Defendants conspired with others to hack into Plaintiffs' computer systems and email servers located in California.

281. The GRA Defendants knowingly received property, including private communications, documents, trade secrets and intellectual property housed on Plaintiffs' and Google's servers, and in emails and documents physically located on those servers located in California.

282. This property was stolen from Plaintiffs in California or otherwise obtained from Plaintiffs in California in a manner that constitutes theft.

283. The GRA Defendants received the property knowing that it was stolen property and obtained through theft. They knowingly and intentionally concealed, sold, withheld—and aided in the concealing, selling and withholding—of Plaintiffs' stolen property.

284. As a direct and proximate result of the actions of the GRA Defendants, Plaintiffs incurred substantial losses and damage, including but not limited to:

(a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;

(b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

(c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;

(d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Mr. Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill; and

(e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation.

285. The total amount of these losses will be proven at trial but, in any event, far exceeds $75,000.

286. The GRA Defendants' conduct has caused, and will continue to cause, Plaintiffs irreparable injury, including loss of goodwill, an increased risk of further theft, and an increased risk of harassment. Plaintiffs have been forced to expend considerable time, money and effort safeguarding their personal information in the wake of these series of hacks. Plaintiffs will continue to suffer this injury as long as their personal information is available to the GRA Defendants, and subsequently, to media organizations and the world at large. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction to return Plaintiffs' stolen property and to refrain from engaging in any conduct described in this Cause of Action.

COUNT SEVEN

(Against all Defendants)

Civil Conspiracy

287. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this Complaint.

288. Defendants agreed to engage in the above-mentioned tortious and criminal actions to harm Mr. Broidy's business and public standing.

289. Defendants willfully, intentionally, and knowingly agreed and conspired with each other and with others, including Qatar and other members of the Qatari-Funded Criminal Enterprise, to engage in the wrongful conduct alleged herein, including but not limited to:

(a) Willfully and intentionally accessing without authorization a facility through which an electronic communication service is provided, namely, BCM's computer systems, including its email servers, and thereby obtaining access to wire or electronic communications while they were in electronic storage in such systems, in violation of 18 U.S.C. § 2701(a);

(b) Intentionally accessing Plaintiffs' and Google's servers, and emails and documents physically located on those servers and accounts, without authorization and then stealing and curating Plaintiffs' data and emails, in violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a) and Cal. Pen. Code § 502;

(c) Willfully, intentionally, and maliciously misappropriating Plaintiffs' trade secrets to benefit the government of Qatar, a foreign power, and the Qatari-Funded Criminal Enterprise, in violation of both the laws of the United States and California;

(d) Knowingly and intentionally receiving stolen property and concealing that property from Plaintiffs, in violation of California law;

(e) Invading Plaintiffs' privacy by publicizing private facts and intruding upon his seclusion;

(f) Tortiously interfering with Plaintiffs' business relationships by using documents and information stolen from Plaintiffs' servers to disparage Plaintiffs' business and conduct.

290. Defendants engaged in numerous overt acts to further their conspiracy, including, but not limited to, hacking Plaintiffs' emails and other electronic documents, and hiring subcontractors and other co-conspirators to facilitate the hacking.

291. Defendants also furthered the conspiracy by intentionally destroying evidence of their misconduct after Mr. Broidy filed his first lawsuit. Defendants intentionally wiped GRA's computers, phones and other devices clean of any damaging evidence; removed certain hard drives, phones and devices with incriminating evidence from GRA's offices; and brought those devices to a remote location where Defendants destroyed them and discarded the remains.

292. Defendants each actively participated in the above-described civil conspiracy, and therefore each Defendant is responsible for each tortious and otherwise illegal action of any co-conspirator.

293. As a direct and proximate result of the actions of Defendants, Plaintiffs incurred substantial losses and damage, including but not limited to:

(a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;

(b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

(c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new

computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;

(d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Mr. Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill; and

(e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation.

294. The total amount of these losses will be proven at trial but, in any event, far exceeds $75,000.

295. This conspiracy is ongoing. Defendants' conduct has caused, and will continue to cause, Plaintiffs irreparable injury, including loss of goodwill, an increased risk of further theft, and an increased risk of harassment. Plaintiffs have been forced to expend considerable time, money and effort safeguarding their personal information in the wake of these series of hacks. Plaintiffs will continue to suffer this injury as long as their personal information is available to Defendants, and subsequently, to media organizations and the world at large. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting Defendants from engaging in this conspiracy, including efforts to destroy evidence of it, and the conduct described in this Cause of Action.

COUNT EIGHT

(Against all GRA Defendants)

Intrusion Upon Seclusion

296. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this First Amended Complaint.

297. Plaintiffs have a legally protected privacy interest in their personal information. This includes their Google login information, their emails, and documents contained on BCM's servers and computer systems. Plaintiffs' email servers and computer systems contained private information and secrets that Plaintiffs had secluded away from public attention and prying eyes.

298. The GRA Defendants conspired with others to purposefully and repeatedly hack Plaintiffs' computer systems and email servers over a period of weeks. In doing so, they intruded upon Plaintiffs' secluded documents and private communications, viewing them through electronic means and then printing them out.

299. Much of the information the GRA Defendants illegally obtained in the hacking concerned Mr. Broidy's private matters and is not of public interest. Defendants' tortious scheme—committing repeated cybercrimes to facilitate the publishing of a private citizen's secrets—is highly offensive and shocking to any reasonable person. Defendants were retained specifically as part of an effort to harm Mr. Broidy's business and public standing. They accomplished that end through illegal means, by stealing and conspiring to publish private facts about his personal life and matters.

300. Defendants intruded upon Mr. Broidy's seclusion between January 16, 2018 and February 25, 2018 and other times within two years of the commencement of this action.

301. The stealing and subsequent public disclosure of misleading and curated information has caused Plaintiffs to suffer monetary damages, at an amount to be proven at trial,

but in any event, in excess of $75,000, exclusive of interest and costs. The injury to Plaintiffs' privacy is ongoing, and thus the damages Plaintiffs seek may not be finally set. Because the GRA Defendants' actions are intolerable in a civilized community, Plaintiffs also seek punitive damages to deter this sort of criminal enterprise behavior.

302. As a direct and proximate result of the actions of the GRA Defendants, Plaintiffs incurred substantial losses and damage, including but not limited to:

(a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;

(b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

(c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;

(d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Mr. Broidy's and other employees' time spent investigating the hacking, taking remedial measures in

response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill; and

(e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation.

303. The total amount of these losses will be proven at trial but, in any event, far exceeds $75,000.

304. The stealing and public disclosure of Plaintiffs' personal information has caused, and will continue to cause, Plaintiffs irreparable injury, including loss of goodwill, an increased risk of further theft, and an increased risk of harassment. Plaintiffs have been forced to expend considerable time, money and effort safeguarding their personal information in the wake of these series of hacks. Plaintiffs will continue to suffer this injury as long as their personal information is available to the GRA Defendants, and subsequently, to media organizations and the world at large. Such injury cannot be adequately compensated by monetary damages. Plaintiffs accordingly seek an injunction prohibiting the GRA Defendants from violating Plaintiffs' privacy or engaging in the conduct described in this Cause of Action.

COUNT NINE

(Against all GRA Defendants)

Violations of RICO Act, 18 U.S.C. § 1962(c) and § 1964

305. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this First Amended Complaint.

306. The federal RICO statue provides, "It shall be unlawful for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or

foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity." 18 U.S.C. § 1962(c).

307. The RICO statute further provides that "Any person injured in his business or property by reason of a violation of section 1962 of this chapter may sue therefor in any appropriate United States district court and shall recover threefold the damages he sustains and the cost of the suit, including a reasonable attorney's fee . . . ." *Id.* § 1964(c).

308. At all relevant times, Plaintiffs and each Defendant are persons within the meaning of 18 U.S.C. §§ 1961(3), 1962(c) and 1964(c).

A. The Qatari-Funded Criminal Enterprise

309. The GRA Defendants are a group of people and entities associated together in fact with several other individuals and entities, including members of the Qatari government, for the common purpose of carrying out an ongoing criminal enterprise, as described in the foregoing paragraphs of this First Amended Complaint (the Qatari-Funded Criminal Enterprise). Specifically, the Enterprise has engaged in a pattern of illegal and covert operations designed to silence and neutralize people who are perceived to be enemies or critics of Qatar.

310. At all relevant times, the Enterprise described herein was engaged in, and its activities affected, interstate and foreign commerce within the meaning of 18 U.S.C. § 1962(c).

311. Together, the GRA Defendants and their co-conspirators form an association-in-fact enterprise within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c). Each Defendant has knowingly, willfully and unlawfully participated in the operation or management of the Enterprise, directly or indirectly, as described in the foregoing paragraphs of this First Amended Complaint and as identified further below.

312. Upon information and belief, the Qatari-Funded Criminal Enterprise consists of, at least, Kevin Chalker, Denis Mandich, Antonio Garcia, GRA LLC, GRA Maven LLC, GRA

Quantum LLC, Global Risk Advisors EMEA Limited, GRA Research LLC, Qrypt Inc., Gregory Howard, Nicolas Muzin, Joseph Allaham, the Emir of Qatar (GRA code name, "Apex"), the Emir's brother, MBH (GRA code name, "Mightier"), MBH's chief of staff (GRA code name, "Shep"), Stonington, BlueFort Public Relations LLC, and numerous other known and unknown individuals, including cyber hackers, public relations professionals, lobbyists, political actors, and other members of the Qatari government.

313. The Defendants and their co-conspirator members of the Enterprise have functioned, and continue to function, as a unit in carrying out their multi-year, ongoing pattern of racketeering activity through a campaign to neutralize critics of Qatar. Defendant Chalker is responsible for oversight and management of the hacking operations that are instrumental to the Enterprise's common purpose. Defendants Mandich and Garcia are key operatives who at times shared oversight and management responsibility with Defendant Chalker. By stealing the types of confidential information that could harm individuals who are perceived to be threats to Qatar, these individuals provide the Enterprise with the necessary content to be manipulated, falsified and widely disseminated to inflict maximum damage on the victim. Through those operations, they manage and/or facilitate the Enterprise's activities. Defendants GRA LLC, GRA Maven LLC, GRA Quantum LLC, Global Risk Advisors EMEA Limited, Qrypt Inc. and GRA Research LLC, on information and belief, are co-conspirator entities that employ hackers who help develop the plans to attack perceived critics of Qatar and ultimately carry out the operations of the Enterprise. They operate as separate but intertwined departments of a single company whose finances are thoroughly comingled. As a result, they also help manage and/or facilitate the Enterprise's activities.

314. Defendants' co-conspirators—including the above-identified lobbyists, public relations firms, and members of the Qatari government—each helped manage and direct different aspects of the Enterprise in pursuit of the same common objective: to silence Qatar's critics. Their specific roles involved identifying individuals who were perceived to be threats to Qatar's standing in the world community; instructing Defendants to conduct cyberattacks on those targets; obtaining the confidential information stolen by Defendants; manipulating and falsifying that content; and then disseminating it widely to members of the national and international media for the purpose of harming Plaintiffs and other victims of Defendants' cyberattacks.

315. On information and belief, all Defendants and their co-conspirators have worked together, and continue to work together, to develop, orchestrate and implement their plans to silence and neutralize individuals who criticize Qatar and thereby threaten its standing in the world community.

316. The Qatari-Funded Criminal Enterprise is an enterprise under the RICO Act that is separate and distinct from Defendants and their co-conspirators. The activities of the Enterprise are separate and distinct from the ordinary and legitimate business operations of the individual Defendant entities and those of their co-conspirator entities, as well as the ordinary business operations of Messrs. Chalker, Mandich and Garcia and other individual participants in the racketeering activity who also happen to work for a Defendant entity and/or serve in an officer, director or beneficiary capacity for such an entity.

317. Defendants and their co-conspirators committed the above and below-described tortious and criminal acts as part of a common purpose to serve the Enterprise. These actions

were separate and distinct from any lawful work they may have performed under contract for Qatar.

318. The Qatari-Funded Criminal Enterprise engaged in tortious conduct that crossed state and international lines, spanning from Qatar to California, New York, and Washington, DC, among other areas. The GRA Defendants used their interstate network of skilled hackers to advance the Enterprise.

319. Plaintiffs hereby allege and set forth the following predicate racketeering activities as defined under 18 U.S.C. § 1961. Defendants jointly and individually committed each separate set of predicate acts alleged below.

B. Pattern of Racketeering Activity

320. The GRA Defendants each participated in the "pattern of racketeering activity" described in the foregoing paragraphs within the meaning of 18 U.S.C. §§ 1961(1) & (5). They committed multiple acts of wire fraud, in violation of 18 U.S.C. § 1343; multiple acts of criminal money laundering, in violation of 18 U.S.C. § 1957; multiple misappropriations of trade secrets, in violation of the Defend Trade Secrets Act, 18 U.S.C. §§ 1832(a)(1) and (a)(5); and multiple acts of economic espionage, in violation of 18 U.S.C. §§ 1831(a)(1) and (a)(5). These predicate acts are not isolated incidents but instead form a continuous, related pattern of racketeering activity with the common purpose of conducting covert and illegal operations to silence and neutralize Qatar's critics.

321. Together, these numerous predicate acts are part of an open-ended, multi-year scheme of racketeering that, on information and belief, continues through the present. The Enterprise has inflicted numerous injuries against many victims over a period of multiple years. Its campaign to silence its critics is ongoing, and it continues to commit acts of racketeering to shield Qatar from public scrutiny. Media organizations are still to this day relying on

information stolen from Mr. Broidy's computer systems and email servers to publish stories to damage his image. For example, media outlets have continued to falsely claim that Mr. Broidy was a target in the investigation of special counsel Robert Mueller into Russian interference in U.S. elections, whereas in reality he was never interviewed by Mueller's team and does not appear once in the Mueller Report. If left unchecked, the Qatari-Funded Criminal Enterprise presents a distinct threat of long-term racketeering activity.

322. Alternatively, the predicate acts outlined herein are part of a multi-year closed-ended scheme of racketeering that ended in late 2018.

1. First Set of Predicate Acts: Wire Fraud, in violation of 18 U.S.C. § 1343

323. Federal law imposes criminal penalties on "[w]hoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice." 18 U.S.C. § 1343.

324. As discussed above, the Qatari-Funded Criminal Enterprise's purpose was to silence Qatar's critics so as to improve its standing in the international community. That effort included the illicit work of Defendants and their co-conspirators to maintain Qatar's status as host of the 2022 World Cup by silencing its critics. The effort continued thereafter in 2014, when Defendants Chalker and GRA LLC actively pitched Qatar as a client for whom they could tackle all manner of political opponents, in direct furtherance of the Enterprise's objective—to silence Qatar's critics. This ultimately included the 2017 hacking of the UAE Ambassador and the 2017-18 hacking of Mr. Broidy. As has been publicly reported in *The New York Times* and

other media outlets, forensic evidence indicates that Qatar, and therefore GRA, were likely involved in targeting over 1,000 people and entities via cyberattacks similar to those deployed against Plaintiffs here, including prominent officials from countries like Egypt and the United Arab Emirates, and an American columnist and political activist, Shmuley Boteach, all of whom are known as outspoken critics of Qatar.[33]

325. As outlined below, these acts in furtherance of the Enterprise included multiple instances of wire fraud.

(a) Silencing Critics of Qatar's Hosting Status for the 2022 World Cup

326. To ensure that Qatar maintained its status as host of the 2022 World Cup, The GRA Defendants conducted "Project Riverbed," a covert operation designed to target some of Qatar's biggest detractors, including Theo Zwanziger, the former president of the German Football Association and a then-current member of FIFA's executive committee. At the time, Mr. Zwanziger actively promoted the idea of taking back Qatar's successful hosting bid and giving it to a different country. The GRA Defendants specifically intended to neutralize Mr. Zwanziger, by targeting and influencing people close to him through covert influence and operations. The assignment included infiltrating FIFA itself.

327. From approximately 2012-2014, the GRA Defendants' work in Project Riverbed specifically involved a covert action program, so-called "black ops," and the use of various IT platforms. They intentionally targeted individuals and entities across multiple continents, set up

[33] *See* Shmuley Boteach, "Qatar's War to Destroy Pro-Israel Jews," Jerusalem Post, Oct. 8, 2018, https://www.jpost.com/Opinion/Qatars-war-to-destroy-pro-Israel-Jews-568942; Eli Lake, "Russian Hackers Aren't the Only Ones to Worry About," Bloomberg, Sept 18, 2018, https://www.bloomberg.com/opinion/articles/2018-09-18/russian-hackers-aren-t-the-only-onesto-worry-about.

and terminated multiple "cover for action" entities in various jurisdictions, and segregated their legal and illegal operations among "white" and "black" offices.

328. The GRA Defendants conducted more hacking and surveillance operations targeting FIFA executive committee members and related parties to gain "predictive intelligence" and "total information awareness." Obtaining "total information awareness" with respect to both professional communications and deeply private information was, in part, done to acquire blackmail- and extortion-type information that could be used to silence targeted individuals.

329. On information and belief, the GRA Defendants intentionally and willfully conducted these operations in order to execute their scheme to defraud the targets through fraudulent representations that the GRA Defendants caused to be transmitted across wires in interstate and/or foreign commerce. In so doing, the GRA Defendants intended for the targets to rely on their false representations to their detriment (and on information and belief, the targets did), and the GRA Defendants contemplated the harm they would cause them. These acts constituted multiple acts of wire fraud. The Qatari government paid the GRA Defendants tens o millions for this work alone.

(b) Hacking the UAE Ambassador

330. The GRA Defendants also furthered the Qatari-Funded Criminal Enterprise by attempting to silence Qatar's political opponents, including the UAE Ambassador to the United States.

331. In or around April and May 2017, approximately a half-year before the GRA Defendants attacked Mr. Broidy, they specifically intended to conduct and did conduct similar cyberattacks against the UAE Ambassador, as part of an organized effort to discredit him and

improve Qatar's image with the United States. As with Mr. Broidy, hacked emails were disseminated to the media in an effort to embarrass the UAE Ambassador.

332. The GRA Defendants' attack against the UAE Ambassador involved a scheme to defraud him through fraudulent representations that the GRA Defendants caused to be transmitted across wires in interstate and/or foreign commerce. In so doing, the GRA Defendants intended for the UAE Ambassador to rely on those false representations and contemplated the harm their attacks would cause him.

333. By way of example, the GRA Defendants deployed tactics designed to defraud the UAE Ambassador and hack his confidential property by using fake messages from Gmail accounts that appeared to be official and using messages that displayed a correct but redacted phone number for him. They intended for the UAE Ambassador to rely on those fraudulent messages to his detriment (and on information and belief, he did). They also deployed evasion tactics to help bypass automatic spam filter and other security alerts and used private registration services and "throw away accounts" from the Mail.Ru group. The GRA Defendants also maintained multiple phishing sites but hosted them on their own dedicated servers, using different subdomains for different campaigns. They attempted to evade discovery by swiftly taking down sites that appeared to have been noticed, redirecting them all to the www.accessdenied.com site (HTTP 302 code).

334. The GRA Defendants intentionally and willfully conducted the above-described operations, designed to defraud the UAE Ambassador so as to hack his confidential information, and thereby committed multiple acts of wire fraud in furtherance of the Enterprise.

(c) Hacking Mr. Broidy and BCM

335. As described in detail above, from December 2017 through February 2018, Defendants engaged in multiple spear phishing attempts, followed by unauthorized access to

Plaintiffs' computers and networks. The spear phishing attempts were efforts to obtain access to Mr. Broidy and BCM's computers and networks, under fraudulent pretenses, so as to steal Plaintiffs' confidential information. The operations were conducted in furtherance of the Enterprise's purpose of silencing Qatar's political opponents.

336. The GRA Defendants sent at least one such fraudulent email to Robin Rosenzweig. On December 27, 2017, she received an email at her Gmail account that appeared to be a security alert from Google. The email used Google trademarks without the permission of Google, including the Google logo and the Gmail logo. It was sent from a Gmail address and had been disguised to look like an authentic security alert from Google. The email purported to alert Ms. Rosenzweig that the security on her account had been compromised and that she needed to verify or change her account credentials.

337. On or around January 14, 2018, the GRA Defendants sent other fraudulent spear phishing emails to Mr. Broidy's Executive Assistant. These emails were disguised as Google security alerts, which bore Google trademarks used without Google's permission, and were sent through Google's Gmail service in violation of Google's Terms of Service and Gmail's Program Policies.

338. One of the fraudulent spear phishing emails contained a fictitious security alert with a picture of the Executive Assistant's face and part of the Executive Assistant's phone number. The email was sent from a misleading Gmail account with the name "Gmail Account" and the email address noreply.user.secure.services@gmail.com, which had been drafted to look like an authentic security alert from Google. The email purported to alert the Executive Assistant that the security on the account had been compromised and that the Executive Assistant needed to verify or change the Google credentials.

339. The GRA Defendants sent numerous spear phishing emails like the ones described above using interstate wires, and these transmissions crossed state lines.

340. The GRA Defendants used the above-described spear phishing emails to make material misstatements with the specific intent that the targeted individuals would rely on those false representations to their detriment and surrender their valuable login credentials so that they could then use those credentials to hack into Plaintiffs' computer systems. The GRA Defendants did so while contemplating the harm that they would cause these targets and ultimately cause Mr. Broidy. They succeeded.

341. Having fraudulently obtained those credentials through material misstatements, The GRA Defendants commenced an illegal cyberattack against Mr. Broidy and BCM's computer systems and servers. These cyber transmissions used interstate wires and crossed state lines—for example, forensic investigation has revealed that some transmissions traveled from Vermont to California. The GRA Defendants and their co-conspirators initiated thousands of intrusions into Plaintiffs' computer systems and email servers.

342. The GRA Defendants thereby obtained Plaintiffs' valuable electronic information, including but not limited to emails, private information, contracts, trade secrets, and business plans. The GRA Defendants launched the spear phishing attempts with the specific intent of fraudulently depriving Plaintiffs of their valuable property.

343. The GRA Defendants each perpetrated several acts of wire fraud by committing and supervising the spear phishing efforts against associates of Mr. Broidy in order to obtain their valuable login credentials to BCM's computer systems and email servers.

344. As detailed above, the GRA Defendants' actions have directly and proximately caused Plaintiffs to suffer injury to their business or property, including (without limitation)

damage resulting from harm to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets and confidential business information; and harm to Plaintiffs' business, in an amount to be proven at trial.

2. Second Set of Predicate Acts: Federal Criminal Money Laundering in Violation of 18 U.S.C. § 1957

345. Under certain defined circumstances, federal law imposes criminal liability on any person who "knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than $10,000 and is derived from specified unlawful activity." 18 U.S.C. § 1957(a). A "monetary transaction" means the "deposit, withdrawal, transfer, or exchange, in or affecting interstate or foreign commerce, of funds or a monetary instrument … by, through, or to a financial institution." 18 U.S.C. § 1957(f)(1). "Criminally derived property" means "any property constituting, or derived from, proceeds obtained from a criminal offense." 18 U.S.C. § 1957(f)(2). The term "specified unlawful activity" includes any act or offense that constitutes "racketeering activity" under 18 USC § 1961(1), such as each of the various predicate acts identified herein. *See* 18 U.S.C. § 1957(f)(3).

346. As outlined above, in furtherance of the Enterprise, the GRA Defendants engaged in a pattern of racketeering activity that included multiple acts of wire fraud. By intentionally and knowingly making multiple fraudulent misrepresentations, the GRA Defendants induced individuals to provide their log-in credentials to Plaintiffs' computers and servers, and the GRA Defendants then used those credentials to hack into and steal Plaintiffs' confidential material. They did the same to the UAE Ambassador. And in the context of holding on to World Cup 2022, they conducted a campaign of covert, black ops using IT platforms. The Qatari

government and/or their agents paid the GRA Defendants millions of dollars for directing and engaging in these criminal acts of wire fraud.

347. On information and belief, these offenses took place in the United States. Alternatively, to the extent certain acts took place outside the United States, the GRA Defendants who conducted those acts were U.S. persons, within the meaning of 18 U.S.C. § 3077.

348. In the fall of 2017, Defendant Kevin Chalker held over $40 million in accounts affiliated with Bernoulli Limited and Toccum Limited, offshore shell companies formed in Gibraltar for which Mr. Chalker served as the sole director. By late 2018, the accounts for both held under $98,000.

349. On information and belief, the GRA Defendants knowingly used portions of their illicit proceeds, valued at greater than $10,000, to pay the individual hackers whom they employed to carry out these complex acts of wire fraud. On information and belief, each of those monetary transactions was by, through or to a financial institution within the meaning of 18 U.S.C. §§ 1956(c)(6) and 1957(f)(1), affected interstate or foreign commerce, and constituted an act of criminal money laundering that forms part of the pattern of racketeering activity in which the GRA Defendants engaged.

3. Third Set of RICO Offenses: Violations of the Defend Trade Secrets Act. 18 U.S.C. §§ 1832(a)(1) and (a)(5)

350. The Defend Trade Secrets Act imposes criminal penalties against anyone who "knowingly . . . with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly . . . steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;. . . [or] without

authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; [or] receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization." 18 U.S.C. § 1832(a).

351. The Defend Trade Secrets Act also imposes criminal penalties on "whoever . . . conspires with one or more other persons" to violate § 1832(a)(1). *Id*. § 1832(a)(5).

352. Through their hacking of Mr. Broidy's and BCM's computers and networks, the GRA Defendants and other members of the Qatari-Funded Criminal Enterprise repeatedly violated the Defend Trade Secrets Act, 18 U.S.C. § 1832, *et seq.* The BCM servers stored trade secrets including but not limited to highly confidential business plans and proposals; research supporting those plans and proposals, including cost proposals and service projections; vendor lists; requests for proposals and responses thereto; information concerning business strategies and opportunities; and contacts for important business relationships. BCM is a sophisticated investment management and services firm that possesses and uses its trade secrets to serve its customers and create a competitive market advantage.

353. Moreover, Plaintiffs' emails contained confidential information involving contracts, business proposals, and cost estimates involving Mr. Broidy's company and its clients. These contracts, proposals, and estimates contained sensitive information about Mr. Broidy's clients and his company's confidential technology and methods.

354. These trade secrets are of substantial value to Plaintiffs, and they were used and intended for use in relation to products and services in interstate and foreign commerce.

355. Plaintiffs take and have taken reasonable measures to keep this information secret. For example, Plaintiffs have always maintained their information on secured servers that are protected by passwords, firewalls, and antivirus software.

356. Plaintiffs' trade secrets derive independent actual and potential economic value from not being generally known or available to the public or other persons who can obtain economic value from their disclosure or use.

357. Plaintiffs' trade secrets have significant value, resulting from significant investment of time and resources.

358. Plaintiffs have made, and continue to make, efforts that are reasonable under the circumstances to maintain the secrecy of their trade secrets.

359. The GRA Defendants each unlawfully and without authorization appropriated, obtained, and stole Plaintiffs' trade secrets. They knew that BCM's servers contained trade secrets and intended to steal them in order to harm Plaintiffs and economically benefit both themselves and Qatar. The GRA Defendants were paid substantial amounts to misappropriate and publish Plaintiffs' trade secrets, and Qatar hoped to use those trade secrets to its economic benefit. The GRA Defendants thereby committed multiple violations of the Defend Trade Secrets Act.

360. The GRA Defendants' knowing and intentional violation of the Defend Trade Secrets Act has materially injured Plaintiffs. It has deprived them of valuable trade secrets, and caused them to expend resources to defend against further cyberattacks.

361. The Qatari-Funded Criminal Enterprise's misappropriation of Plaintiffs' trade secrets began in January of 2018 and is ongoing.

362. As detailed above, the GRA Defendants' actions have directly and proximately caused Plaintiffs to suffer injury to their business or property, including (without limitation) damage resulting from harm to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets and confidential business information; and harm to Plaintiffs' business, in an amount to be proven at trial.

4. Fourth Set of Predicate Acts: Economic Espionage, in Violation of 18 U.S.C. §§ 1831(a)(1) and (a)(5)

363. Federal law provides that "[w]hoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret . . . [or] (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization" violates 18 U.S.C. § 1831(a)(1).

364. Federal law also imposes penalties on "[w]hoever . . . conspires with one or more other persons to commit" a violation of § 1831(a)(1). *Id*. § 1831(a)(5).

365. The GRA Defendants each unlawfully and without authorization took, appropriated, and obtained Plaintiffs' trade secrets through the cyberattack against Plaintiffs' computers and servers. The GRA Defendants and other members of the Qatari-Funded Criminal Enterprise knew that BCM's servers contained trade secrets and intended to steal them in order to harm Plaintiffs. They misappropriated Plaintiffs' trade secrets intentionally for the benefit of their foreign client, Qatar, and acted with the knowledge that their actions would have the effect of benefiting the foreign nation of Qatar.

366. The GRA Defendants used an artifice and fraud—the fake Gmail spear phishing emails—in order to take, appropriate, and obtain Plaintiffs' trade secrets.

367. The GRA Defendants used fake spear phishing emails to induce targets to surrender their valuable login credentials. Multiple targets did provide their login credentials in reliance on these false material statements.

368. As detailed above, Defendants' actions have directly and proximately caused Plaintiffs to suffer injury to their business or property, including (without limitation) damage resulting from harm to Plaintiffs' computers, servers, and accounts; loss in the value of Plaintiffs' trade secrets and confidential business information; and harm to Plaintiffs' business, in an amount to be proven at trial.

C. Summary of the Pattern of Racketeering Activity as to Each Defendant

369. The Qatari-Funded Criminal Enterprise has engaged in a pattern of racketeering activity with relationship and continuity in pursuit of a common purpose: to silence Qatar's critics. As outlined below, each of the GRA Defendants knowingly, intentionally and willfully participated in the operation and management of the Enterprise by engaging in at least two predicate acts of racketeering in furtherance of that objective. The GRA Defendants are each directly and primarily liable for multiple acts of wire fraud, money laundering, misappropriation of trade secrets, and economic espionage.

1. Defendant Kevin Chalker

370. Mr. Chalker, as a former CIA intelligence officer and the founder and CEO of Global Risk Advisors LLC, directly managed and conducted all aspects of the cyberattacks described in this First Amended Complaint. He personally solicited and obtained Qatar as a client and conspired with others to perform multiple predicate acts of wire fraud, money laundering, violations of the Defend Trade Secrets Act and economic espionage, all in furtherance of the Enterprise's objective to silence and neutralize Qatar's critics and enemies.

371. Mr. Chalker conspired with the other GRA Defendants, as well as his other co-conspirators in the Enterprise, to use his unique expertise and skillset to develop, plan and launch the cyberattacks described herein, and to synchronize those attacks with the work of lobbyists and public relations professionals so as to inflict maximum damage on Mr. Broidy and the other victims.

372. Mr. Chalker developed very close relationships with his co-conspirator members of the Qatari government and their agents, including the Emir, giving them code names of "Shep," "Mightier" and "Botany." He worked closely and conspired with all of these individuals over a period of several years to devise, manage and execute the attacks described herein in furtherance of the Enterprise's objective.

373. Mr. Chalker's work in furtherance of the Enterprise included his and his co-conspirators multiple intentional and willful acts of wire fraud and money laundering, outlined above, to ensure that Qatar held on to hosting the 2022 World Cup.

374. His work for the Enterprise continued in 2014, when he spearheaded the effort to assist Qatar in neutralizing their political opponents in the international community.

375. And he carried out that effort in at least 2017 and 2018 when he directed, managed and conducted the above-described cyberattacks on the UAE Ambassador and Mr. Broidy and BCM.

376. In connection with those attacks, Mr. Chalker intentionally and willfully committed multiple acts of wire fraud, money laundering, violations of the Defend Trade Secrets Act, and economic espionage.

2. Defendant Denis Mandich

377. Defendant Denis Mandich, a 20-year veteran of the intelligence community, joined GRA no later than 2017 and co-founded Qrypt Inc. with Kevin Chalker.

378. Mr. Mandich conspired with the other Defendants, as well as his other co-conspirators in the Enterprise, to use his unique expertise and skillset to develop, plan and launch the cyberattacks against the UAE Ambassador and Plaintiffs, as described herein, and to synchronize those attacks with the work of lobbyists and public relations professionals so as to inflict maximum damage on Mr. Broidy and the other victims.

379. In connection with those attacks, Mr. Mandich intentionally and willfully committed multiple acts of wire fraud, money laundering, violations of the Defend Trade Secrets Act, and economic espionage.

3. Defendant Antonio Garcia

380. Defendant Antonio Garcia, who served as GRA's Chief Security Officer, was affiliated with GRA LLC, and in particular, its Reston Group.

381. Mr. Garcia conspired with the other Defendants, as well as his other co-conspirators in the Enterprise, to use his unique expertise and skillset to develop, plan and launch the cyberattacks against the UAE Ambassador and Plaintiffs, as described herein, and to synchronize those attacks with the work of lobbyists and public relations professionals so as to inflict maximum damage on Mr. Broidy and the other victims.

382. Mr. Garcia also played a key part in destroying evidence of the Defendants' misconduct. After Plaintiffs filed their first lawsuit, Mr. Garcia wiped GRA's computers, phones and other devices clean of any damaging evidence of the cyberattacks. He also removed certain hard drives, phones and devices with incriminating evidence from GRA's offices, and brought them to a remote location, where the devices were destroyed and ultimately discarded. Upon information and belief, Defendant Courtney Chalker knowingly assisted Mr. Garcia with the destruction of evidence.

383. In connection with the cyberattacks and subsequent destruction of evidence, Mr. Garcia intentionally and willfully committed multiple acts of wire fraud, money laundering, violations of the Defend Trade Secrets Act, and economic espionage.

4. Defendant GRA LLC

384. Defendant GRA LLC is a limited liability company formed under the laws of Delaware and founded by Mr. Chalker. Its primary place of business is in New York, New York, and it has a branch office in Washington, DC.

385. GRA LLC wholly owns (a) Defendant Global Risk Advisors EMEA Limited, a Gibraltar corporation, which began to operate in Doha, Qatar on October 26, 2017; (b) Defendant GRA Maven, a military consulting firm which was founded by Mr. Chalker in 2016 and which is headquartered in Southern Pines, North Carolina; and (c) Defendant GRA Quantum, a full-service cybersecurity company which was founded by Mr. Chalker in 2015, and which maintains an office in New York, New York.

386. GRA LLC is one of several entities that Mr. Chalker used to facilitate the multiple predicate acts of wire fraud, money laundering, violations of the Defend Trade Secrets Act and economic espionage outlined herein. It employs highly skilled hackers, many of whom are former US intelligence officers and military personnel who have a specialized background and expertise in the intelligence community, black ops, and other covert operations. GRA LLC and its employees directly participated in planning and executing all of the cyberattacks outlined herein, including those related to protecting Qatar's status as host of the 2022 World Cup, and the attacks on UAE Ambassador and Mr. Broidy and BCM. It managed and directed the activities of sophisticated hackers and cyber-firms, and it had substantial decision-making authority and discretion to conduct the cyberattacks described herein.

5. Defendant GRA Maven LLC

387. GRA Maven, a military consulting firm based in North Carolina, is owned by GRA LLC and is another entity that Mr. Chalker used to facilitate the multiple predicate acts of wire fraud, money laundering, violations of the Defend Trade Secrets Act and economic espionage outlined herein. On information and belief, it also employs highly skilled hackers, many of whom are former US intelligence officers and military personnel who have a specialized background and expertise in black ops and other covert operations. GRA Maven and its employees directly participated in the attacks on the UAE Ambassador and Mr. Broidy and BCM.

388. Specifically, in connection with the attacks on Mr. Broidy and BCM, Defendants used another IP address traced to the North Carolina Research and Education Network ("NCREN") and a server in Chapel Hill, North Carolina—close to GRA Maven's Southern Pines, North Carolina offices—to deposit the PDF formatted electronic documents into the "LA.Confidential@mail.com" during this time. NCREN provides broadband infrastructure to various public institutions in North Carolina, and the particular IP address at issue is associated with a "guest" Wi-Fi network at the University of North Carolina. This point of access for the conspirators' email is roughly an hour's drive from both GRA Maven's location and from the towns where GRA employees lived at that time. On information and belief, GRA Maven and its employees participated in this aspect of the attacks on Mr. Broidy and BCM and thus intentionally and willfully committed multiple acts of wire fraud, money laundering, violations of the Defend Trade Secrets Act and economic espionage. It managed and directed the activities of sophisticated hackers and cyber-firms, and it had substantial decision-making authority and discretion to conduct the cyberattacks described herein.

6. Defendant GRA Quantum LLC

389. GRA Quantum LLC is a full-service cybersecurity company owned by GRA LLC and founded by Mr. Chalker in 2015. It maintains an office in New York, New York. It is another entity that Mr. Chalker used to facilitate the multiple predicate acts of wire fraud, money laundering, violations of the Defend Trade Secrets Act and economic espionage outlined herein. On information and belief, it also employs highly skilled hackers, many of whom are former US intelligence officers and military personnel who have a specialized background and expertise in black ops and other covert operations. GRA Quantum LLC and its employees directly participated in the attacks on the UAE Ambassador and Mr. Broidy and BCM and thus intentionally and willfully committed multiple acts of wire fraud, money laundering, violations of the Defend Trade Secrets Act and economic espionage. It managed and directed the activities of sophisticated hackers and cyber-firms, and it had substantial decision-making authority and discretion to conduct the cyberattacks described herein. It recently launched an affiliate company called Legato Security, incorporated in Utah days after GRA Quantum was added as a Defendant in this case on December 27, 2019.

7. Defendant Global Risk Advisors EMEA Limited

390. Defendant Global Risk Advisors EMEA Limited ("GRA EMEA"), a Gibraltar corporation, is also owned by GRA LLC and is another entity that Mr. Chalker used to facilitate the multiple predicate acts of wire fraud, money laundering, violations of the Defend Trade Secrets Act and economic espionage outlined herein. It currently has operations based in Doha, Qatar.

391. At Mr. Chalker's direction, GRA EMEA and its employees conspired with members of the Qatari government to conduct "special projects" that involved spying on Americans in furtherance of the Enterprise's objectives. This work was segregated even within

GRA because Mr. Chalker, GRA EMEA, its employees, and its co-conspirators well knew that the special projects involved extensive criminal conduct, including the predicate acts described above.

392. In or around mid-August 2017, Qatar and GRA EMEA reached an agreement on a broad cybersecurity and surveillance arrangement. On information and belief, the agreement called for GRA to work directly with Qatar's Special Forces and intelligence collection agencies, including on cybersecurity, surveillance and countersurveillance.

393. In October 2017, during the planning stages of the upcoming attack on Mr. Broidy and BCM, Mr. Chalker registered a branch of GRA EMEA—the Qatar Financial Centre Branch—in Doha, Qatar. And in March 2019, GRA EMEA was registered in Qatar. Qatari corporate records list its directors as Mr. Chalker and Daniel Emory.

394. On information and belief, GRA EMEA intentionally and willfully committed multiple acts of wire fraud, money laundering, violations of the Defend Trade Secrets Act and economic espionage. It managed and directed the activities of sophisticated hackers and cyber-firms, and it had substantial decision-making authority and discretion to conduct the cyberattacks described herein.

8. Defendant GRA Research LLC

395. Defendant GRA Research, LLC d/b/a Tactical Data Analytics is a limited liability company formed under the laws of Delaware with an office at the same Washington, DC address as Defendant GRA LLC. It has also had a branch registered in Virginia since 2014, as well as an office in or near Reston, VA. Upon information and belief, GRA Research LLC is under common ownership with the other the GRA entities, and ultimately controlled by Defendant Chalker. Defendant Antonio Garcia, who served as GRA's Chief Security Officer, was also affiliated with GRA Research LLC.

396. While GRA had hackers in a number of locations, many of the GRA hackers working on the campaign against Plaintiffs were located in GRA Research LLC's offices in Northern Virginia. GRA broadly employed many former intelligence and military personnel with offensive hacking skills developed while in government service, with a large team in Northern Virginia that was referred to as the "Reston Group" and affiliated with GRA Research LLC. The Reston Group was centrally involved in many "special projects" hacking operations, including the hack of Plaintiffs.

397. The head of the Reston Group was a former CIA official with information security expertise. Other members in the Reston Group included a software engineer formerly with the military, a former member of the Army's special operations forces, and others with prior work experience in cyberwarfare. The Group included one particularly trusted operative, Defendant Anthony Garcia, who was GRA's Chief Security Officer and who, shortly after Mr. Broidy filed his first lawsuit arising from the hacks, electronically "wiped" and then physically destroyed the electronic evidence in Northern Virginia and New York related to the hacking.

398. GRA Research LLC is another entity that Mr. Chalker used to facilitate the multiple predicate acts of wire fraud, money laundering, violations of the Defend Trade Secrets Act and economic espionage outlined herein. GRA Research LLC and its employees directly participated in the attacks on the UAE Ambassador and Mr. Broidy and BCM and thus intentionally and willfully committed multiple acts of wire fraud, money laundering, violations of the Defend Trade Secrets Act and economic espionage. It managed and directed the activities of sophisticated hackers and cyber-firms, and it had substantial decision-making authority and discretion to conduct the cyberattacks described herein.

9. Defendant Qrypt Inc.

399. Defendant Qrypt Inc., a Delaware-incorporated and New York-based full-service cybersecurity company, was founded by Defendants Kevin Chalker and Denis Mandich in the fall of 2017, days after EMEA entered into a broad cybersecurity and surveillance contract with Qatar during the planning stages of the attack on Plaintiffs. Both Messrs. Chalker and Mandich are veterans of the intelligence community with extensive cybersecurity experience. In 2019, in connection with his work for Qrypt, Defendant Mandich authored two cybersecurity patents.

400. On information and belief, Qrypt, Inc. is another entity that Mr. Chalker used to facilitate the multiple predicate acts of wire fraud, money laundering, violations of the Defend Trade Secrets Act and economic espionage outlined herein. On information and belief, it also employs highly skilled hackers, many of whom are former US intelligence officers and military personnel who have a specialized background and expertise in black ops and other covert operations. Qrypt, Inc. and its employees directly participated in the attacks on Mr. Broidy and BCM and thus intentionally and willfully committed multiple acts of wire fraud, money laundering, violations of the Defend Trade Secrets Act and economic espionage. It managed and directed the activities of sophisticated hackers and cyber-firms, and it had substantial decision-making authority and discretion to conduct the cyberattacks described herein.

D. Effect on Interstate Commerce

401. The Qatari-Funded Criminal Enterprise has substantially affected interstate commerce by (1) committing multiple acts of wire fraud and money laundering involving transactions that cross state and international lines, as described above; and (2) causing damage to Plaintiffs and other victims of these attacks by harming property and business, including loss of valuable electronic information, business plans, contracts, vendor lists, requests for proposals, consumer good will, and substantial expense in protecting Plaintiffs' and other victims'

computer systems and email servers from additional cyberattack. Plaintiffs (and the other victims of these attacks, including, for example, Theo Zwanziger and the UAE Ambassador) regularly conduct business in interstate commerce, and Defendants' cyber-hacking has substantially disrupted that business.

E. Business Injury

402. As a direct and proximate result of Defendants' racketeering activity, Plaintiffs incurred substantial and concrete financial loss and damage to their business and property, including but not limited to:

(a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;

(b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

(c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;

(d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Mr. Broidy's and other employees' time spent investigating the hacking, taking remedial measures in

response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill; and

(e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation.

403. The GRA Defendants' racketeering activity has further directly and proximately caused loss to Plaintiffs' business by deliberately and foreseeably harming the confidence and trust of its existing and potential clients in Plaintiffs' ability to maintain the security and secrecy of client data. Plaintiffs' business involves sensitive work in the government contract space where discretion and security are critical. A highly public hacking scheme like this one has naturally caused significant lost revenue and other harm. In other words, Defendants' racketeering activity has directly and proximately caused damage to Plaintiffs' goodwill and business relationships, causing loss to the value of Plaintiffs' business and lost profits, among other damages.

404. Plaintiffs are entitled to treble damages and attorneys' fees under 18 U.S.C. § 1964(c).

COUNT TEN

(Against all GRA Defendants)

Conspiracy to Violate RICO Statute, 18 U.S.C. § 1962(d)

405. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph of this First Amended Complaint.

406. The RICO Act provides that "[i]t shall be unlawful for any person to conspire to violate any of the provisions" of the Act. 18 U.S.C. § 1962(d).

407. The GRA Defendants knowingly and voluntarily agreed with other members of the Qatari-Funded Criminal Enterprise to engage in the above-mentioned racketeering activity with the common objective of silencing Qatar's critics. In so doing, they intentionally and willfully conspired to commit, and ultimately committed, the above-described predicate acts.

408. Defendants Kevin Chalker and GRA LLC knew about and agreed to participate in the conspiracy when they began their collective and illicit efforts to help Qatar hold on to hosting World Cup 2022. All the GRA Defendants knew about and agreed to participate in the conspiracy many years ago, when their criminal operations described above were first launched.

409. The GRA Defendants and other members of the Qatari-Funded Criminal Enterprise committed the above-referenced racketeering acts in furtherance of their racketeering conspiracy.

410. The GRA Defendants each committed numerous acts of racketeering knowingly in furtherance of the conspiracy, including wire fraud, money laundering, misappropriation of trade secrets, and economic espionage.

411. As a direct consequence and by reason of the GRA Defendants' racketeering conspiracy, Plaintiffs have suffered injury to their business and property, which includes, but is not limited to, concrete financial loss, discussed above.

412. These injuries to Plaintiffs' business and property were the natural, foreseeable, and intended result of the GRA Defendants' RICO conspiracy and the acts committed in furtherance thereof.

413. Plaintiffs are entitled to treble damages and attorneys' fees under 18 U.S.C. § 1964(c).

PRAYER FOR RELIEF

414. Plaintiffs repeat and re-allege the allegations contained in each and every preceding paragraph of this Complaint.

415. Wherefore, Plaintiffs request that this Court order the following relief against Defendants:

(a) Grant judgment in favor of Plaintiffs and against Defendants as to all Causes of Action;

(b) Declare that Defendants' conduct constitutes violations of the statutes and common law cited herein;

(c) Award Plaintiffs an appropriate amount in monetary damages as determined at trial, including but not limited to pre- and post-judgment interest and treble damages under RICO, 18 U.S.C. § 1964 and Cal. Pen. Code § 496;

(d) Grant all appropriate injunctive relief against Defendants, disgorgement of unjust riches, constructive trust over Plaintiffs' trade secrets and other materials, and any other equitable relief deemed appropriate;

(e) Award Plaintiffs punitive damages under 18 U.S.C. § 2707, and Cal. Pen. Code § 502, and Plaintiffs' common-law causes of action, as well as exemplary damages under Cal. Civ. Code § 3426.3, and 18 U.S.C. § 1836(b)(3)(C);

(f) Award Plaintiffs attorneys' fees and the costs of bringing this action; and

(g) Grant Plaintiffs such other relief as is just and appropriate.

JURY DEMAND

Plaintiffs hereby demand a trial by jury.

Respectfully Submitted,

STEPTOE & JOHNSON LLP

/s/ Filiberto Agusti
Filiberto Agusti
Leah M. Quadrino
Linda C. Bailey
1330 Connecticut Avenue, NW
Washington, DC 20036
Phone: (202) 429-3000
Fax: (202) 429-3902
fagusti@steptoe.com
lquadrino@steptoe.com
lbailey@steptoe.com

Charles Michael
Morgan Lucas
1114 Avenue of the Americas
New York, NY 10036
Phone: (212) 506-3900
Fax: (202) 506-3950
cmichael@steptoe.com
mlucas@steptoe.com

Counsel for Plaintiffs Elliott Broidy and Broidy Capital Management LLC

Dated: June 26, 2020